

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

#1703  
11-25-A  
JC557 U.S. PTO  
09/037916  
03/10/98

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application: 1997年10月 1日

出 願 番 号

Application Number: 平成 9年特許願第268891号

出 願 人

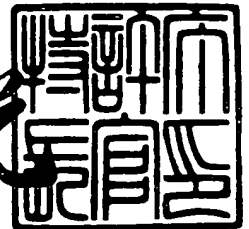
Applicant (s): 富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

1997年12月19日

特許庁長官  
Commissioner,  
Patent Office

荒井寿光



【書類名】 特許願

【整理番号】 9704230

【提出日】 平成 9年10月 1日

【あて先】 特許庁長官殿

【国際特許分類】 G07F 7/08  
G06F 15/30  
G06K 17/00

【発明の名称】 二重財布を有する電子財布システム、その電子財布システムに適用される ICカード、二重財布を有する ICカード取引装置、二重財布を有する ICカード取引システムおよびその ICカード取引システムに適用される ICカード

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 西尾 信彦

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 麻生 泉

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 二重財布を有する電子財布システム、その電子財布システムに適用されるＩＣカード、二重財布を有するＩＣカード取引装置、二重財布を有するＩＣカード取引システムおよびそのＩＣカード取引システムに適用されるＩＣカード

【特許請求の範囲】

【請求項１】 第１預金額が格納される第１領域と第２預金額が格納される第２領域とを備えた書き換え可能な第１不揮発性メモリと、当該メモリに接続された処理装置と、当該処理装置の動作プログラムを格納した第２不揮発性メモリと、当該処理装置を介して前記第１、第２不揮発性メモリにそれぞれ格納された情報にアクセスするための入力端子を備えた携帯型のカード状担体であって、

前記第１不揮発性メモリの第１領域に対応して少なくともカード所有者の個人認証番号が前記第１不揮発性メモリに格納され、

前記第１不揮発性メモリの第２領域に対応して当該第２領域へのアクセスを許容できる装置の種類を示す識別情報が前記第１不揮発性メモリに格納され、

前記第１領域へのアクセスに際して前記入出力端子から入力され暗号化された情報を解読し、その解読された情報に含まれる暗証番号と前記第１不揮発性メモリに格納された個人認証番号とが所定の関係である場合にアクセスを許容し、

前記第２領域へのアクセスに際してアクセスする取引装置の種類を示す識別番号が一致する場合、前記第２領域へのアクセスを許容するカード状担体と、

預金額が格納された口座ファイルを有するセンタシステムと、

前記カード状担体のメモリの第１領域に、前記センタシステムの預金額の一部または全部を移送するための前記センタシステムに直接または間接的に連携された引出装置であって、

装置の識別情報と、カード所有者が入力した暗証番号の内、少なくとも一方を暗号化して前記カード状担体に転送する引出装置と、

暗証番号および前記カード状担体における前記第１領域から前記第２領域に転送すべき金額を入力する入力手段と、前記カード状担体に対して前記入力手段によって入力された暗証番号と転送金額と識別情報とを供給する転送装置と、

前記カード状担体の第2領域に格納された預金額を使用するため、利用金額と装置情報とを送出する利用装置と、

を備え、

前記カード状担体は、

前記転送装置によって転送を指示され、かつ前記個人認証番号が許容された場合には、前記第1領域に格納された預金額を指定された金額分減算して前記第1領域の更新を行うとともに、前記第2領域に指定された金額を書き込み、

前記利用装置により利用金額を指示され、かつ前記識別情報が前記第2領域へのアクセスを許容された場合には、前記利用金額を減算して前記利用装置での前記利用金額の利用を許容することを特徴とする二重財布を有する電子財布システム。

【請求項2】 前記カード状担体は、前記第2不揮発性メモリに前記第2領域が引出処理のみ許容するプログラムを格納していることを特徴とする請求項1に記載の二重財布を有する電子財布システム。

【請求項3】 前記カード状担体は、前記第1不揮発性メモリに第3領域を有し、前記第3領域には、当該第3領域へのアクセスを許容する利用装置の識別情報および暗証番号が登録され、前記第2不揮発性メモリには、前記利用装置から登録されている情報に対応する識別情報および暗証情報が入力された場合に前記第3領域の加算又は減算を許容するプログラムが格納されていることを特徴とする請求項1に記載の電子財布システム。

【請求項4】 前記カード状担体は、前記第3領域に、加算処理した前記利用装置を示す識別情報と加算処理した額とを履歴情報として格納することを特徴とする請求項3に記載の二重財布を有する電子財布システム。

【請求項5】 前記カード状担体は、前記利用装置が前記第1不揮発性メモリの領域を指定せずに支払い処理を要求した際に、前記利用装置からの転送情報の復号化処理をスキップして、前記第2預金額から指定された金額情報を差し引く取引を許容することを特徴とする請求項2に記載の二重財布を有する電子財布システム。

【請求項6】 第1金額が記憶された第1財布、第2金額が記憶された第2

財布、支払い処理プログラム、利用者の暗証番号プログラムを格納したメモリと

前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、

外部装置と通信を遂行する通信手段と、

を備えた二重財布を有する電子財布システムに適用されるＩＣカードであって

前記支払いプログラムは、

外部の支払い要求装置から、財布を指定せずに支払いコマンドを受信した場合、前記第２財布に格納された第２金額に基づき支払い処理し、前記第１財布を指定した支払いコマンドを受信した場合、暗証照合を行い、前記第１財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする二重財布を有する電子財布システムに適用されるＩＣカード。

【請求項７】 第１金額が記憶された第１財布、第２金額が記憶された第２財布、支払い処理プログラムおよび暗号化／復号化プログラムを格納したメモリと、

前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、

外部装置と通信を遂行する通信手段と、

外部の取引装置とのインタフェースを司るインタフェース手段と、

を備えた二重財布を有する電子財布システムに適用されるＩＣカードであって

前記支払いプログラムは、

前記インタフェース手段を通じて外部装置から第１財布を指定せずにコマンドを受信した場合、前記第２財布に格納された第２金額に基づいて支払い処理を遂行し、前記第１財布を指定した支払いコマンドを受信した場合、前記暗号化および復号化プログラムを使用して、外部の装置と通信し、前記第１財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする二重財布を有する電子財布システムに適用されるＩＣカード。

【請求項 8】 ICカードに格納される金額とセンタ口座に格納される金額との内の一方を選択し、その選択された金額に基づいて現金支払いを行う ICカード取引装置であって、

ICカードの装着を検出する検出手段と、

前記検出手段により前記 ICカードの装着が検出された後に任意のモード指定を受け付ける受付手段と、

前記受付手段において前記 ICカードの挿入が検出されてから一定時間が経過しても任意のモード指定を受け付けなかった場合に前記センタ口座から現金支払いのための支払いモードに移行するモード移行手段と、

を備えたことを特徴とする ICカード取引装置。

【請求項 9】 第 1 財布と第 2 財布とを有する ICカードを使用して支払い取引を行う取引装置であって、

前記取引装置は、

前記第 1 財布を指定して支払い要求額を入力した際に、暗号化および暗証による支払い承認処理後、前記第 1 財布に格納された金額が取引要求金額に満たない場合、前記第 2 財布に格納された金額を補填して取引を遂行することを特徴とする取引装置。

【請求項 10】 第 1 財布と第 2 財布とを備え、前記第 1 財布と第 2 財布とによる二重財布を用いて取引装置と取引を行う ICカード取引システムに適用される ICカードであって、

前記取引装置から暗証番号とを受信した場合には、前記受信された暗証番号により個人認証処理を行った後、前記取引装置に対して前記第 1 財布と第 2 財布に格納される各金額を出力し、一方、前記取引装置から暗証番号を受信しなかった場合には、前記取引装置に対して前記第 2 財布の金額を出力することを特徴とする二重財布を有した ICカード取引システムに適用される ICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ICカードを利用して電子現金を取り扱う電子財布システムおよ

びそのＩＣカード、二重財布を有するＩＣカード取引装置、ならびに、二重財布を有するＩＣカード取引システムおよびそのＩＣカードに関する。

【０００２】

【従来の技術】

近年、ＩＣカードに書き換え可能な不揮発性メモリとマイクロコンピュータ（マイコン）を内蔵させたＩＣカードが普及し、一方、金融機関の間でこのＩＣカードに銀行口座の預金額をこのＩＣカードを転送させてＩＣカード担体で銀行取引や商店での商品購入ができるいわゆる電子財布システムが各種提唱されている。

【０００３】

従来の電子財布システムでは、一般にＩＣカードには、財布は一つ設けられ、その財布へ端末を通じて希望の金額を引き下ろしたり、あるいは、その財布から端末を通じて支払いをするという形態になっている。そして、ＩＣカードの電子財布には、安全性を高めるために高度のセキュリティ機能が一般的には付与され、このために実際の取引処理をする際に操作の遅延や、処理の遅延があった。

【０００４】

特に、従来の電子財布システムの場合、ＩＣカード内の１つのメモリ領域を外部の装置がアクセスする場合、カード所有者の暗証番号をカード内で照合して認証し、また、装置の識別コードを入力して、そのメモリ領域に対してアクセスが許容されている装置であるかどうか照合してはじめて該当領域へのアクセスが許容されるという所謂、照合処理を行うという仕組みになっている。

【０００５】

また、セキュリティを上げるために、ＩＣカードと端末との間のデータ転送の際は、データを暗号化して転送しているが、これらの暗号化手法として公開キーや秘密キーをそれぞれの装置とＩＣカードとが持ち、場合によってはキーを取引処理の都度、両者の間で交換した後、データを暗号化するという、所謂認証処理が採用されている。この暗号化手法としては、ＲＳＡ方式、ＤＥＳ方式等、装置とＩＣカードに共通の鍵データを持ったり、公開鍵、秘密鍵をそれぞれが持ち、共通のアルゴリズムで送信データを暗号化し、復号化するという手法があり、一



般に採用されている。一方、ICカードの利用は各所で考えられている。一般商店やスーパーマーケット等におけるPOS (Point Of Sale) システム、病院等におけるカルテシステム、パチンコ等の遊技場における遊技システム、競馬等の投票券システム、公衆電話機や交通等の切符システム等、多岐に亘っている。

【0006】

この種の近似技術として、例えば特開平2-205933号公報がある。この公報によれば、自動販売機や店舗における商品購入時の支払いをキャッシュレスで行うためにICカードを用いたシステムが開示されている。具体的には、システムに使用されるICカードのメモリに、プリペイドエリアとオフライン口座エリアとが設けられている。一方のプリペイドエリアは、残高を記憶しておき、PIN (Personal Identification Number) を用いてその残高で現金取引を行うために使用されるエリアである。他方のオフライン口座エリアは、オフライン口座としての残高を記憶しておき、プリペイドエリアの残高を増額するために個人認証番号を用いてその残高をプリペイドエリアに移動させるために使用されるエリアである。

【0007】

【発明が解決しようとする課題】

上記公報のように従来例によるICカードシステムでは、電子財布システムに連携させたシステムが各種提案されているが、いずれもICカードに設けられた一つの電子財布からPINなどを用いての一定の認証処理や一定の照合処理を経由して、暗証照合が成立した場合にのみメモリへのアクセスが可能となった。しかるに、これらのシステムでは、ICカードの不正な捨得の際の安全対策が上述した暗号化技術によって強化されているため、電子財布システムと他のシステムとを連携するには、以下に述べる問題があった。

【0008】

まず、それぞれの利用装置にそれらの認証処理や照合処理のための入力機能を設ける必要があり、セキュリティ上、利用装置側の構成が複雑化していた。

【0009】

また、各システムの利用装置を取り扱う人等、利用装置の所有者或いは、そのソフトウェアの関係者にくまなくシステム全体で使用している共通の暗号化のためのアルゴリズムやキー等が判明してしていた。これにより、各所有者による不正がシステム全体のアクセスを可能にすることから、セキュリティを保持することが不可能であった。それゆえ、システム全体では大きな金額の不正の可能性があり、安全性の面で広い地域や1枚のカードの多面的な利用、所謂マルチユースで利用することが難しかった。

## 【0010】

また、利用者側からみると、前述した公報（特開平2-205993号公報）のように取引時にPINを入力する等、すべての利用に際して暗証番号の入力が必要となるため、操作が煩雑であった。また、システム上、上述した照合処理が存在するため、実際に取引が終了するまでに処理はかなりの時間を要していた。このように、取引時間が必要以上にかかりすぎると、例えば、スーパーマーケットでの混雑時の利用、投票券システムにおける出走直前での券購入時の利用、切符システムにおける出発間際の切符購入等の利用等、緊急時の取引処理での利用が阻害されることになった。

## 【0011】

また、遊技場等における利用の際は、内心は当日の使用金額をあらかじめ決めていたとしても、いつの間にか財布に入っている全額を使い切ってしまうという問題が指摘されているが、現状では、電子財布に入っている金額はすべて使用できることから、電子財布の利用金額を制限することは不可能であった。

## 【0012】

この発明は、ICカードの二重財布としての特性を生かし、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることが可能な二重財布を有する電子財布システムを提供することを第1の目的とする。

## 【0013】

この発明は、第1目的を提供する電子財布システムに適用される二重財布すな

わちＩＣカードを提供することを第２の目的とする。

【００１４】

この発明は、二重財布であるＩＣカード上でのセキュリティを一層向上させることが可能な二重財布を有するＩＣカード取引装置を提供することを第３の目的とする。

【００１５】

この発明は、二重財布（ＩＣカード）としての特性を生かし、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させるカード取引を実現することが可能な二重財布を有するＩＣカード取引システムを提供することを第４の目的とする。

【００１６】

この発明は、第４の目的を提供するＩＣカード取引システムに適用される二重財布すなわちＩＣカードを提供することを第５の目的とする。

【００１７】

【課題を解決するための手段】

上述した課題を解決し、各目的を達成するため、まず、請求項１の発明に係る二重財布を有する電子財布システムは、第１預金額が格納される第１領域と第２預金額が格納される第２領域とを備えた書き換え可能な第１不揮発性メモリと、当該メモリに接続された処理装置と、当該処理装置の動作プログラムを格納した第２不揮発性メモリと、当該処理装置を介して前記第１、第２不揮発性メモリにそれぞれ格納された情報にアクセスするための入力端子を備えた携帯型のカード状担体であって、前記第１不揮発性メモリの第１領域に対応して少なくともカード所有者の個人認証番号が前記第１不揮発性メモリに格納され、前記第１不揮発性メモリの第２領域に対応して当該第２領域へのアクセスを許容できる装置の種類を示す識別情報が前記第１不揮発性メモリに格納され、前記第１領域へのアクセスに際して前記入出力端子から入力され暗号化された情報を解読し、その解読された情報に含まれる暗証番号と前記第１不揮発性メモリに格納された個人認証番号とが所定の関係である場合にアクセスを許容し、前記第２領域へのアクセス

に際してアクセスする取引装置の種類を示す識別番号が一致する場合、前記第2領域へのアクセスを許容するカード状担体と、預金額が格納された口座ファイルを有するセンタシステムと、前記カード状担体のメモリの第1領域に、前記センタシステムの預金額の一部または全部を移送するための前記センタシステムに直接または間接的に連携された引出装置であって、装置の識別情報と、カード所有者が入力した暗証番号の内、少なくとも一方を暗号化して前記カード状担体に転送する引出装置と、暗証番号および前記カード状担体における前記第1領域から前記第2領域に転送すべき金額を入力する入力手段と、前記カード状担体に対して前記入力手段によって入力された暗証番号と転送金額と識別情報とを供給する転送装置と、前記カード状担体の第2領域に格納された預金額を使用するため、利用金額と装置情報とを送出する利用装置と、を備え、前記カード状担体は、前記転送装置によって転送を指示され、かつ前記個人認証番号が許容された場合には、前記第1領域に格納された預金額を指定された金額分減算して前記第1領域の更新を行うとともに、前記第2領域に前記指定された金額を書き込み、前記利用装置により利用金額を指示され、かつ前記識別情報が前記第2領域へのアクセスを許容された場合には、前記利用金額を減算して前記利用装置での前記利用金額の利用を許容することを特徴とする。

## 【0018】

この請求項1の発明によれば、転送装置を用いた取引の場合、暗証番号を用いた個人認証を通じてカード状担体の第1領域（第1財布）から第2領域（第2財布）への預金額の転送を行い、利用装置を用いた取引の場合、個人認証を必要とせずに、カード状担体の第2領域で利用金額を利用するようにしたので、二重財布（ＩＣカード）としての特性が生かされ、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることが可能である。

## 【0019】

また、請求項1の発明は、請求項2のように、カード状担体の第2不揮発性メモリに第2領域が引出処理のみ許容するプログラムを格納するようにしてもよい。

【0020】

また、請求項1の発明は、請求項3の発明のように、カード状担体に設けた第3領域に当該第3領域へのアクセスを許容する利用装置の識別情報および暗証番号を登録しておき、利用装置から登録されている情報に対応する識別情報および暗証情報が入力された場合に第3領域の加算又は減算を許容するようにしてもよい。

【0021】

また、請求項3の発明は、請求項4の発明のように、カード状担体の第3領域に、加算処理した利用装置を示す識別情報と加算処理した額とを履歴情報として格納するようにしてもよい。

【0022】

また、請求項5の発明に係る二重財布を有する電子財布システムは、請求項2の発明において、前記カード状担体は、前記利用装置が前記第1不揮発性メモリの領域を指定せずに支払い処理を要求した際に、前記利用装置からの転送情報の復号化処理をスキップして、前記第2預金額から指定された金額情報を差し引く取引きを許容することを特徴とする。

【0023】

この請求項5の発明によれば、利用装置が領域指定せずに支払い処理を要求した場合には、第2領域の預金額を用いて、セキュリティの低い、個人認証を伴わない簡易な利用取引きを実現することが可能である。

【0024】

また、請求項6の発明に係る二重財布を有する電子財布システムに適用されるICカードは、第1金額が記憶された第1財布、第2金額が記憶された第2財布、支払い処理プログラム、利用者の暗証番号プログラムを格納したメモリと、前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、外部装置と通信を遂行する通信手段と、を備えた二重財布を有する電子財布システムに適用されるICカードであって、前記支払いプログラムは、外部の支払い要求装置から、財布を指定せずに支払いコマンドを受信した場合、前記

第2財布に格納された第2金額に基づき支払い処理し、前記第1財布を指定した支払いコマンドを受信した場合、暗証照合を行い、前記第1財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする。

## 【0025】

この請求項6の発明によれば、外部から財布の指定がなかった場合には第2財布に格納された第2金額に基づき支払いを行い、外部から第1財布が指定された場合には暗証照合を行ってから第1財布での支払いを行うようにしたので、セキュリティの低い第2財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第1財布については個人認証により不正防止を図ることが可能である。

## 【0026】

また、請求項7の発明に係る二重財布を有する電子財布システムに適用されるICカードは、第1金額が記憶された第1財布、第2金額が記憶された第2財布、支払い処理プログラムおよび暗号化／復号化プログラムを格納したメモリと、前記メモリに格納された支払い処理プログラムに従って支払い処理を実行する処理回路と、外部装置と通信を遂行する通信手段と、外部の取引装置とのインタフェースを司るインタフェース手段と、を備えた二重財布を有する電子財布システムに適用されるICカードであって、前記支払いプログラムは、前記インタフェース手段を通じて外部装置から第1財布を指定せずにコマンドを受信した場合、前記第2財布に格納された第2金額に基づいて支払い処理を遂行し、前記第1財布を指定した支払いコマンドを受信した場合、前記暗号化および復号化プログラムを使用して、外部の装置と通信し、前記第1財布に格納された金額に基づいて前記外部装置に対して支払い処理を遂行することを特徴とする。

## 【0027】

この請求項7の発明によれば、外部から財布の指定がなかった場合には第2財布に格納された第2金額に基づき支払いを行い、外部から第1財布が指定された場合には暗号化および復号化を通じて第1財布での支払いを行うようにしたので、セキュリティの低い第2財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第1財布については暗号利用により不

正防止機能を一層向上させることが可能である。

【0028】

また、請求項8の発明に係るICカード取引装置は、ICカードに格納される金額とセンタ口座に格納される金額との内的一方を選択し、その選択された金額に基づいて現金支払いを行うICカード取引装置であって、ICカードの装着を検出する検出手段と、前記検出手段により前記ICカードの装着が検出された後に任意のモード指定を受け付ける受付手段と、前記受付手段において前記ICカードの挿入が検出されてから一定時間が経過しても任意のモード指定を受け付けなかった場合に前記センタ口座から現金支払いのための支払いモードに移行するモード移行手段と、を備えたことを特徴とする。

【0029】

この請求項8の発明によれば、取引装置とICカードとの取引で、一定時間内に任意のモード指定を受け付けた場合にセンタ口座の利用を許し、受け付けられなかった場合には現金支払いに以降するようにしたので、センタ口座の取引についてはモードによるバリエーションを持たせ、現金での取引についてはその指定操作を省くことで、現金取引の簡略化を実現することが可能である。

【0030】

また、請求項9の発明に係る取引装置は、第1財布と第2財布とを有するICカードを使用して支払い取引を行う取引装置であって、前記取引装置は、前記第1財布を指定して支払い要求額を入力した際に、暗号化および暗証による支払い承認処理後、前記第1財布に格納された金額が取引要求金額に満たない場合、前記第2財布に格納された金額を補填して取引を遂行することを特徴とする。

【0031】

この請求項9の発明によれば、取引装置とICカードとの個人認証を要する取引で、第1財布だけで金額上の取引が成立しなくても第2財布の金額を補填して再度取引を遂行するようにしたので、利用者が取引のための金額を気にすることなく取引を遂行することができ、操作性の向上を図ることが可能である。

【0032】

この請求項10の発明に係るICカード取引システムに適用されるICカードは、第1財布と第2財布とを備え、前記第1財布と第2財布とによる二重財布を用いて取引装置と取引を行うICカード取引システムに適用されるICカードであって、前記取引装置から暗証番号とを受信した場合には、前記受信された暗証番号により個人認証処理を行った後、前記取引装置に対して前記第1財布と第2財布に格納される各金額を出力し、一方、前記取引装置から暗証番号を受信しなかった場合には、前記取引装置に対して前記第2財布の金額を出力することを特徴とする。

## 【0033】

この請求項10の発明によれば、取引装置とICカードとの取引で、個人認証を経た場合にのみ第1財布および第2財布の金額を取引装置に出力し、そうでない場合には第2財布の金額のみ取引装置に出力するようにしたので、照会などで財布の中身を取引装置に教える程度の取引であっても、個人認証を通過できなければセキュリティの高い第1財布を開くことを防止することが可能である。

## 【0034】

## 【発明の実施の形態】

以下に添付図面を参照して、この発明に係る二重財布を有する電子財布システム、その電子財布システムに適用されるICカード、二重財布を有するICカード取引装置、二重財布を有するICカード取引システムおよびそのICカード取引システムに適用されるICカードの好適な実施の形態を詳細に説明する。

## 【0035】

まず、システム構成について説明する。図1はこの発明の実施の形態による電子財布システム（ICカード取引システム含む）の一例を示す構成図である。図1に示した電子財布システムは、ICカード1、ICカード1との取引装置である引出装置2、ICカード1との取引装置である利用装置4、センタシステム3より構成される。

## 【0036】

ICカード1は、取引の際に暗証番号（PINの意味）および暗号化を必要とするセキュリティの高い第1財布1Aと取引の際に暗証番号および暗号化を必要



としないセキュリティの低い第2財布1Bとからなる二重財布機能を有している。引出装置2は、ICカード1を着脱自在とした構成であり、銀行などのセンタシステム3との通信を通じて引き出した預金をICカード1の第1財布1Aに格納する。

## 【0037】

センタシステム3は、銀行などのように利用者の預金を管理しており、引出装置2などの機器との通信を通じて預金の引き落としなどを行う。利用装置4は、ICカード1を着脱自在とした構成であり、ICカード1の第2財布1Bに格納された金額で各種のサービスを提供する。

## 【0038】

つぎに、ICカード1について詳述する。まず、原理について説明する。図2は図1に示したICカード1を機能的に示すブロック図である。図2に示したICカード1は、機能として、要求領域識別部11、復号化セキュリティ処理部12、暗証番号処理部13、照合処理部14、アクセス権確認処理部15および取引処理部16を備えている。

## 【0039】

要求領域識別部11は、端末に自ICカード1が装着された際に、第1財布1Aや第2財布1Bの領域を要求しているか、もしくはいずれの領域についても要求していないかを識別する。この要求領域識別部11は、領域要求がない場合に照合処理部14に処理を移す。復号化セキュリティ処理部12は、要求領域識別部11で領域を要求している場合に端末から暗号化されて受信される情報を、復号化キーを使用して復号化する。

## 【0040】

復号化暗証番号処理部13は、暗証番号による個人認証処理を行う。照合処理部14は、自ICカード1を装着した端末がアクセスしてよい端末か否かを照合する。アクセス権確認処理部15は、照合結果からアクセス権の有無を確認する。取引処理部16は、アクセス権有りの確認後に相手端末との間で取引を行う。

## 【0041】

続いて上述したICカード1の原理を実現するハードウェア構成について説明する。図3は図1に示したICカード1をハードウェア的に示すブロック図である。図3に示したICカード1は、相手端末と接続するための端子101、相手端末と自ICカード1内部とのインタフェースを司るインタフェース(I/F)102、CPU103、ROM104、RAM105、EEPROM106等により構成される。

#### 【0042】

CPU103は、ROM104に格納されたプログラムに従って全体の処理を制御する。ROM104は、後述する図8～図17のフローチャートに従うプログラムを格納している。RAM105は、CPU103のワークエリアとして使用される。

#### 【0043】

EEPROM106は、不揮発性メモリであり、前述した第1財布1A、第2財布1Bそれぞれの機能を実現するために使用される第1財布エリア106A、第2財布エリア106Bと、相手端末との取引履歴を記録するために使用される第3財布エリア106Cとを有している。

#### 【0044】

つぎに、上述したICカード1の二重財布構造について説明する。図4は図3に示したICカード1のメモリ構成例を示す図である。ICカード1の二重財布構造は、第1財布エリア106Aと第2財布エリア106Bとで形成される。具体的には、ICカード1のEEPROM106は、図4(a)に示したディレクトリ領域と図4(b)に示したデータ領域とに区分される。

#### 【0045】

ディレクトリ領域は、図4(a)に示したように、第1財布エリア106Aの第1ディレクトリD1、第2財布エリア106Bの第2ディレクトリD2、第3財布エリア106Cの第3ディレクトリD3とにより構成される。

#### 【0046】

第1ディレクトリD1は、第1財布エリア106Aのアドレス(第1財布アドレス)、要求時のセキュリティのためのPINである暗証番号、および相手端末

の機械IDとそのアクセス権との対により構成される。図4(a)の例では、第1財布アドレスは“F001~F00F”、暗証番号は“1234”、機械IDおよびアクセス権は相手端末#1, #2にそれぞれ対応して任意に設定される。アクセス権としては、書き込み、読み出し、更新、消去などがある。

## 【0047】

第2ディレクトリD2は、第2財布エリア106Bのアドレス(第2財布アドレス)、その設定をフリーとする暗証番号、および相手端末の機械IDとそのアクセス権との対により構成される。図4(a)の例では、第2財布アドレスは“F011~F01F”、暗証番号はフリー、機械IDおよびアクセス権は相手端末に対応して任意に設定される。

## 【0048】

第3ディレクトリD3は、第3財布エリア106Cのアドレス(第3財布アドレス)、要求時のセキュリティのためのPINである暗証番号、および相手端末の機械IDとそのアクセス権との対により構成される。図4(a)の例では、第3財布アドレスは“F021~F03F”、暗証番号は“1234”、機械IDおよびアクセス権は相手端末#1, #2にそれぞれ対応して任意に設定される。

## 【0049】

そして、図4(b)に示したデータ領域は、第1財布エリア106A, 第2財布エリア106B, 第3財布エリア106C, 追加情報としてのセンタ口座情報に区分される。

## 【0050】

第1財布エリア106Aに関して、第1ディレクトリD1の第1財布アドレスにより領域が特定され、第1財布としての残金が格納される。第2財布エリア106Bに関して、第2ディレクトリD2の第2財布アドレスにより領域が特定され、第2財布としての残金が格納される。第3財布エリア106Cに関して、第3ディレクトリD3の第3財布アドレスにより領域が特定され、第3財布として第1財布と第2財布の合計額、取引履歴(取引日, 取引機械ID, 取引金額等)等が格納される。なお、センタ口座情報には、センタシステム3における口座番号などの情報が含まれている。

## 【0051】

つぎに、図1に示した引出装置2について詳述する。図5は図1に示した引出装置2を機能的に示すブロック図である。図5に示した引出装置2は、装置識別IDレジスタ21、認証転送処理部22、暗号化処理部23、入力部24により構成される。

## 【0052】

機械IDレジスタ21は、ICカード1が機械を識別できるように機械毎に割り当てられた機械IDを格納している。認証転送処理部22は、センタシステム3から預金を引き出す際に暗証番号および引出金額から認証を行って引出金額を暗号化処理部23に転送する。暗号化処理部23は、機械IDレジスタ21に格納された機械IDや入力部24で入力された暗証番号を暗号化してICカード1に送信する。入力部24は、利用者の手操作により暗証番号や引出金額を入力してこれら入力情報を認証転送処理部22に送出する。

## 【0053】

つぎに、図1に示したセンタシステム3について詳述する。図6は図1に示したセンタシステム3を概略的に示す構成図である。図6に示したセンタシステム3は、引出装置2などに回線で接続されたホストコンピュータ31、各預金者の口座情報を記録したデータベース32などにより構成される。

## 【0054】

ホストコンピュータ31は、データベース32をアクセスして、引出装置2などから預金の引き落とし等の処理を行う。データベース32は、ホストコンピュータ31からアクセスされ、ホストコンピュータ31の要求に応じて所要の口座から預金の一部もしくは全部を引出すなどの処理を行う。

## 【0055】

つぎに、図1に示した利用装置4について詳述する。図7は図1に示した利用装置4を機能的に示すブロック図である。図7に示した利用装置4は、機械IDレジスタ41、転送処理部42、支払額発生部43、取引処理部44、受信部45、メモリ46により構成される。

## 【0056】

機械IDレジスタ41は、ICカード1が機械を識別できるように機械毎に割り当てられた機械IDを格納している。転送処理部42は、特に引出装置2のような認証を必要とせず、サービスを受けるのに必要な支払い額を支払額発生部43から受け取ってICカード1に転送する。また、転送に当たっては暗号化処理は行わない。支払額発生部43は、サービスを提供するのに必要な支払い額を発生して、その支払い額を転送処理部42と取引処理部44とに送出する。

## 【0057】

取引処理部44は、ICカード1からの要求に応じてサービス提供のための支払い額に応じた取引処理を実行する。受信部45は、ICカード1の装着によりサービスに必要な支払い額を受け取り、その通知を取引処理部44に送出するとともに、サービスの履歴情報をメモリ46に送出する。メモリ46は、受信部45からICカード1の履歴情報を受け取って記憶する。

## 【0058】

つぎに、上述した電子財布システムの動作について説明する。まず、ICカード1の動作について説明する。図8および図9は実施の形態によるICカード1のメイン動作を説明するフローチャートである。なお、すでにICカード1は、相手端末（引出装置2もしくは利用装置4）に装着されているものとする。

## 【0059】

具体的には、ICカード1は、まず、相手端末との間で前処理を実行する（ステップS101）。この前処理は、ICカード1を利用できる端末かどうかを相手端末との交信により確認するものであり、その詳細は後述（図16および図17）する。続いて、相手端末よりコマンド受信が行われ（ステップS102）、その受信されたコマンドに第1財布エリア106Aもしくは第2財布エリア106Bを要求する領域IDが含まれているか否か判断される（ステップS103）。なお、この受信コマンドには、機械IDとアクセス権との対などが含まれているが、領域IDについては任意に設定される。

## 【0060】

ステップS103において、もし領域IDが含まれていると判断された場合には、処理はステップS104に移行し、一方、含まれていないと判断された場合

には、処理はステップS112（図9参照）に移行する。

【0061】

まず、処理がステップS104に移行した場合には、受信コマンドに含まれている領域IDから第1財布エリア106Aと第2財布エリア106Bとのいずれの領域が要求されているかを読み取る処理が実行される。さらに受信コマンドに含まれている機械IDとICカード1のEEPROM106に格納されている機械IDとの比較が行われ、両機械IDが一致していれば、処理はステップS106に移行し、一方、一致していなければ、このICカード1は相手端末を利用できないものとして処理は無効とされる（ステップS105）。

【0062】

ステップS106では、EEPROM106に機械IDと対で記憶されているアクセス権と受信コマンドに含まれるアクセス権（受信アクセス）との対応が確認される。その結果、両アクセス権が対応していると判断された場合には、処理はステップS107に移行するが、対応していないと判断された場合には、このICカード1は相手端末をアクセスできないものとして処理は無効とされる。

【0063】

ステップS107では、ステップS104で読み取られた領域が第1財布エリア106Aであった場合には、続くステップS108において相手端末からの要求内容が判別され、一方、第2財布エリア106Bであった場合には、他モードとして処理が実行される。

【0064】

ステップS108において、要求内容が転送であれば、処理はステップS109に移行して転送処理（図10、図11参照）を実行し、支払いであれば、処理はステップS110に移行して支払い処理（図12および図13参照）を実行し、カード預金であれば、処理はステップS111に移行してカード預金処理（図15および図16参照）を実行する。以上の転送処理、支払い処理、カード預金処理のいずれかが終了した後に、本処理は終了する。

【0065】

また、ステップS103で受信コマンドに領域IDが含まれていなかった場合

には、強制的に支払いモードとしての処理が開始される。まず、ステップS112（図9参照）において、強制的にEEPROM106の第2ディレクトリD2にある第2財布アドレスが読み出される。そして、同第2ディレクトリD2に格納される機械IDが受信コマンド中の機械IDと比較され、一致していれば、処理はステップS114に移行するが、一致していなければ、このICカード1は相手端末を利用できないものとして処理は無効とされる。

【0066】

ステップS114では、ステップS112で読み出した第2財布アドレスから第2財布エリア106Bに格納されているデータすなわち残高が読み込まれる。続いてその読み込まれた第2財布エリア106Bの残高は相手端末に出力される（ステップS115）。この残高の出力により相手端末側では、第2財布に入っている金額を知ることが出来る。そして、ICカード1に対して要求額（支払い額）を含んだ支払いコマンドが出力される。

【0067】

続いて、相手端末から一定時間内に支払いコマンドが受信されると（ステップS116）、続くステップS117において第2財布エリア106Bに格納されている残高から相手端末が支払いを要求する金額すなわち要求額が差し引かれる。その結果得られた金額はRAM105にあらかじめ設けられたワークエリアW1に格納される。なお、ステップS116において支払いコマンドの受信がなかった場合には、相手端末との支払い取引はなかったものとして処理は終了する。

【0068】

そして、このワークエリアW1に格納された金額がゼロもしくはプラスであれば（ステップS118）、第2財布だけで相手端末が要求する支払いが可能であることから、相手端末に対して、支払い可としてその支払い可の情報と支払い額（要求額を意味する）とが通知される（ステップS119）。なお、ステップS118においてワークエリアW1の金額がマイナスを示していた場合には、相手端末との支払い取引はなかったものとして処理は終了する。

【0069】

ステップS119において通知が行われた後、一定時間が経過しても相手端末からその通知に対する応答が行われなかった場合には（ステップS120）、ワークエリアW1に格納された金額はクリアされ、相手端末との支払い取引きはなかったものとして処理は終了する。一方、一定時間内に相手端末から応答受信が入った場合には（ステップS120）、その応答受信から受け取りコードが受信される（ステップS121）。

#### 【0070】

このように、相手端末から受け取りコードが受信されると、その相手端末において支払いに応じた処理が実行されたことになるため、第2財布エリア106Bの残高が更新される。すなわち、ワークエリアW1の金額が第2財布エリア106Bに格納され（ステップS122）、併せてその支払い取引の日付が第3財布エリア106Cに履歴として格納される（ステップS123）。最後に、相手端末に対してICカード1内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップS124）。

#### 【0071】

つぎに、上述したメイン動作の個々の動作について説明する。まず、転送処理（図8のステップS109）について説明する。図10および図11は図8に示したメイン動作における転送処理を説明するフローチャートである。この転送処理は、ICカード1が引出装置2に装着された場合を想定しており、引出装置2を用いて残金が不足している第2財布に対して第1財布に入っている残金の一部（転送要求額）を転送するものである。この転送処理には、第1財布のセキュリティ上、PINである暗証番号および暗号化／復号化の処理が必要となる。

#### 【0072】

この転送処理では、まず、相手端末からの転送要求額が受信され、その転送要求額が復号される（ステップS1001）。続いて、第1財布エリア106Aに格納された残高から復号された転送要求額が差し引かれ、その金額がRAM105にあらかじめ設けておいたワークエリアW2に格納される（ステップS1002）。このワークエリアW2に格納された金額は、第1財布から第2財布に転送要求額を転送したと仮定した場合の第1財布の残高を示している。



## 【0073】

ここでは、第1財布へのアクセスとなり、転送取引きそのものが高度なセキュリティを伴うことから、暗証番号による個人認証が必要となる。そのため、相手端末に対して暗証番号が要求される（ステップS1003）。この後、相手端末から暗証番号が送信されるまで一定時間受信待ちとなる（ステップS1004）。なお、一定時間を経過しても暗証番号が受信されない場合には、図示せぬがこの転送取引きは終了する。

## 【0074】

そして、相手端末から暗証番号が受信され（ステップS1004）、ステップS1002でワークエリアW2に格納された金額がゼロもしくはプラスであった場合には（ステップS1005）、ステップS1004で受信された暗証番号が復号される（ステップS1006）。一方、ワークエリアW2に格納された金額がマイナスであった場合には（ステップS1005）、この転送取引きはなかったものとして無効にされる。

## 【0075】

ステップS1006で暗証番号が復号されると、続くステップS1007において、第1ディレクトリD1に格納されている暗証番号が読み出され、その暗証番号が復号される。そして、この復号されたICカード1自身の暗証番号と相手端末から受け取って復号した暗証番号との照合が行われ（ステップS1008）、両暗証番号が一致した場合には（ステップS1009）、認証および照合をパスできたものとして処理はステップS1010に移行する。一方、認証および照合をパスできなかった場合には、この転送取引きはなかったものとして無効にされる。

## 【0076】

ステップS1010では、第2財布エリア106Bに格納されている金額（残高）に転送額（前述の転送要求額）が加算され、その合計がワークエリアW1に格納される。このワークエリアW1に格納された金額は、第1財布から第2財布に転送額を転送したと仮定した場合の第2財布の残高を示している。

## 【0077】

続いて、この転送取引では認証および照合のパスに応じて転送可となることから、ワークエリアW1、W2に格納された金額がそれぞれ暗号化される（ステップS1011）。このようにして暗号化された各金額は暗号化情報として相手端末に送信される（ステップS1012）。

#### 【0078】

その後、相手端末から一定時間内に応答受信がない場合には（ステップS1013）、処理はステップS1014に移行して、この転送取引はなかったものにするため、ワークエリアW1、W2はいずれもクリアされる。その後、処理はメイン処理（図8参照）に戻る。一方、ステップS1013において応答受信が確認された場合には、その応答受信によって受信されたデータが了解コードか否か判断される（ステップS1015）。この了解コードは、相手端末において利用者が要求する転送の了解を意味するものである。

#### 【0079】

ステップS1015において受信データが了解コードであった場合には、転送取引が成立したものとして、まずワークエリアW2の暗号化された金額が第1財布エリア106Aに格納され（ステップS1017）、さらにワークエリアW1の暗号化された金額が第2財布エリア106Bに格納される（ステップS1018）。このようにして、第1財布エリア106Aと第2財布エリア106Bとは、転送要求金額に従って残高が更新される。なお、ステップS1015において受信データが了解コードでなかった場合には、転送取引が成立しないものとして、続くステップS1016において相手端末にコメント再送要求が行われ、処理はメインのステップS102（図8参照）に戻る。

#### 【0080】

さらに、第3財布エリア106Cには、上述した転送取引の日付などの情報が履歴として格納される（ステップS1019）。最後に、相手端末に対してICカード1内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップS1020）。

#### 【0081】

続いて、支払い動作（図8のステップS110）について説明する。図12お

よび図13は図8に示したメイン動作における支払い処理を説明するフローチャートであり、図14は図12に示した支払い処理における追加取引を説明するフローチャートである。この支払い処理は、ICカード1が引出装置2に装着された場合を想定しており、引出装置2を用いて第1財布に入っている残金の一部（転送要求額）を引出装置2に支払うものである。この支払い処理には、第1財布のセキュリティ上、PINである暗証番号が必要となる。

#### 【0082】

この支払い処理では、まず、相手端末に対して暗証番号および要求額が要請される（ステップS1101）。その後、暗証番号および要求額が受信されると（ステップS1102）、まず要求額が復号される（ステップS1003）。続いて、第1財布エリア106Aに格納された残高から復号された要求額が差し引かれ、その金額がRAM105のワークエリアW2に格納される（ステップS1004）。このワークエリアW2に格納された金額は、第1財布から引出装置2に要求額を支払ったと仮定した場合の第1財布の残高を示している。

#### 【0083】

そして、ステップS1104でワークエリアW2に格納された金額がゼロもしくはプラスであった場合には（ステップS1105）、今度はステップS1102で受信された暗証番号が復号される（ステップS1107）。一方、ワークエリアW2に格納された金額がマイナスであった場合には（ステップS1105）、処理はステップS1106に移行して追加取引（図14参照）を実行する。

#### 【0084】

ステップS1107で暗証番号が復号されると、続くステップS1108において、第1ディレクトリD1に格納されている暗証番号が読み出され、その暗証番号が復号される。そして、この復号されたICカード1自身の暗証番号と相手端末から受け取って復号した暗証番号との照合が行われ（ステップS1109）、両暗証番号が一致した場合には（ステップS1110）、認証をパスできたものとして処理はステップS1111に移行する。一方、認証をパスできなかった場合には、この支払い取引はなかったものとして無効にされる。

#### 【0085】

ステップS1111では、この支払い取引では認証のパスに応じて支払い可となることから、ワークエリアW2に格納された金額が暗号化される。このようにして暗号化された金額は暗号化情報として相手端末に送信される（ステップS1112）。

【0086】

その後、相手端末から一定時間内に応答受信がない場合には（ステップS1113）、処理はステップS1115に移行して、この支払い取引はなかったものにするため、ワークエリアW2はクリアされる。その後、処理はメイン処理（図8参照）に戻る。一方、ステップS1113において応答受信が確認された場合には、その応答受信によって受信されたデータが受け取りコードか否か判断される（ステップS1114）。この受け取りコードは、相手端末において利用者が要求する支払いの受け取り完了を意味するものである。

【0087】

ステップS1114において受信データが受け取りコードであった場合には、支払い取引が成立したものとして、ワークエリアW2の暗号化された金額が第1財布エリア106Aに格納される（ステップS1116）。このようにして、第1財布エリア106Aは、支払い要求金額に従って残高が更新される。

【0088】

さらに、第3財布エリア106Cには、上述した転送取引の日付などの情報が履歴として格納される（ステップS1117）。最後に、相手端末に対してICカード1内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップS1118）。

【0089】

さて、上述したステップS1106による追加取引（図14参照）はつぎのように処理される。すなわち、まず、ステップS1501において第2財布エリア106Bの残高が読み出され、続くステップS1502においてその読み出された残高がすでにステップS1104でワークエリアW2に格納された金額に加算される。すなわち、この合計によりワークエリアW2の格納額が更新される。

【0090】

そして、ステップS11502で更新されたワークエリアW2の格納額がゼロもしくはプラスであった場合には（ステップS1503）、処理はステップS1504に移行するが、ワークエリアW2の格納額がマイナスであった場合には（ステップS1503）、第1財布の残高に第2財布の残高を加算しても支払要求額を満たせないことから、この支払い取引はなかったものとして無効にされる。

#### 【0091】

処理がステップS1504に移行すると、第1財布の残高に第2財布の残高を加算した額が支払要求額を満たすことから、支払い可としての処理が続行される。そのために、処理は前述したステップS1107に戻り、同様の処理を実行する。ただし、この追加取引を含むことで第2財布エリア106Bの残高が使用されたことから、ステップS1116では、この追加取引を含む場合にのみ第2財布エリア106Bの格納額がゼロにクリアされる。

#### 【0092】

さらに続いてカード預金処理（図8のステップS111）について説明する。図15および図16は図8に示したメイン動作におけるカード預金処理を説明するフローチャートである。このカード預金処理は、引出装置2を利用してセンタシステム3から預金を要求額分だけ引出し、その引き出した要求額をICカード1に格納する処理である。このカード預金処理には、第1財布のセキュリティ上、PINである暗証番号が必要となる。

#### 【0093】

まず、相手端末に対して預金要求額を要求し、その相手端末から送られてくる預金要求額を復号する処理が実行される（ステップS1201）。この預金要求額は相手端末において預金者が入力する情報である。続いてEEPROM106のデータ領域からセンタ口座情報が読み出され、そのセンタ口座情報に含まれる口座番号が抽出される（ステップS1202）。

#### 【0094】

続いて、相手端末に対して暗証番号が要求され（ステップS1203）、その後、相手端末から暗号化された暗証番号が受信されると、その暗号化された暗

証番号は復号される（ステップS1204）。そして、第1財布の暗証番号が第1ディレクトリD1より読み出され（ステップS1205）、その暗証番号が復号される（ステップS1206）。

【0095】

さらに、相手端末から送られてきた領域IDからセンタ転送用暗号化キーが読み出され（ステップS1207）、そのセンタ転送用暗号化キーを用いてステップS1201で復号された預金要求額とステップS1202で読み出された口座番号とが暗号化される（ステップS1208）。このようにして暗号化された情報は暗号化情報としてカード預金要求コマンドに付加されてセンタ送信される（ステップS1209）。

【0096】

その後、センタシステム3から要求額が送られてくるまで処理は受信待ちとなる（ステップS1210）。センタシステム3から要求額が送られてくると（ステップS1211）、第1財布エリア106Aに格納されている残高が読み取られる（ステップS1212）。この第1財布の残高に受信された要求額が加算され、その合計がワークエリアW2に格納され（ステップS1213）、そのワークエリアW2の格納額が第1財布エリア106Aに格納される。これにより、第1財布エリア106Aへのカード預金が完了する。

【0097】

そして、要求額、第1財布エリア106Aの残高がそれぞれ暗号化され（ステップS1215）、その暗号化された情報（暗号化情報）が相手端末に出力される（ステップS1216）。

【0098】

つぎに、前述の電子財布システムにおいて実施される復号、暗号化、前処理について説明する。まず、復号処理について説明する。図17は実施の形態における復号処理を説明するフローチャートである。

【0099】

図17に示した復号処理は、電子財布システムに適用される引出装置2、利用装置4、ICカード1にすべて付加される機能である。その機能は、図示せぬが

、DSP (Digital Signal Processor) により実現してもよい。このDSPを適用する場合には、そのDSP内に復号のための復号回路部が設けられる。

【0100】

動作としては、まず、領域IDから復号キーが読み出され（ステップS1301）、DSPの復号回路部へその復号キーが送信される（ステップS1302）。相手端末からの受信データから復号部が抽出され（ステップS1303）、その抽出された復号部が復号回路部へ転送される（ステップS1304）。このようにして復号回路部には、復号キーと復号部とが揃うので、その段階で復号回路部において復号が行われる。そして、復号回路部からの復号データが受信されると、復号処理は完了する（ステップS1305）。

【0101】

続いて暗号化処理について説明する。図18は実施の形態における暗号化処理を説明するフローチャートである。図18に示した暗号化処理は、電子財布システムに適用される引出装置2、利用装置4、ICカード1にすべて付加される機能である。その機能は、図示せぬが、DSP (Digital Signal Processor) により実現してもよい。このDSPを適用する場合には、そのDSP内に復号のための暗号回路部が設けられる。

【0102】

動作としては、まず、領域IDから暗号化キーが読み出され（ステップS1401）、DSPの暗号回路部へその暗号化キーが送信される（ステップS1402）。相手端末からの受信データから暗号化すべきデータが抽出され（ステップS1403）、その抽出されたデータが暗号回路部へ転送される（ステップS1404）。このようにして暗号回路部には、暗号化キーと暗号化すべきデータとが揃うので、その段階で暗号回路部において暗号化が行われる。そして、暗号回路部からの暗号化データが受信されると、暗号化処理は完了する（ステップS1405）。

【0103】

さらに続いて前処理について説明する。図19および図20は実施の形態にお

ける前処理を説明するフローチャートである。以下に説明する図19および図20では、端末側とICカード1間の通信処理が示されている。

【0104】

端末は、まず、ICカード1の挿入待ちとなり（ステップT1）、一定時間毎に挿入状態が確認される（ステップT2）。ICカード1が端末の装着部に挿入されると、端末はその挿入からICカード1のセット状態を確認する（ステップT2）。その後、端末は、ICカード1に電源を供給し（ステップT3）、さらにリセット信号を送信する（ステップT4）。

【0105】

ICカード1は、端末から電源供給を受けた後に自身の電源をONし（ステップC1）、続いて送られてくるリセット信号に従ってCPU103をリセットする（ステップC2）。その後、ICカード1は初期化などを経て、まず自ICカード1で利用できる商用カードの種類（例えばVISAカード、マスターカードなど）を読み出す（ステップC3）。その読み出されたカード種類はATR（Answer To Reset）信号に付加されて相手端末に返信される（ステップC4）。

【0106】

端末は、リセット信号を送信した後にカード種類を受け取ると（ステップT4）、そのカード種類から自端末で利用できるカードを識別する（ステップT5）。なお、利用できるカードがない場合には、この取引は強制終了される。また、利用できるカードがあれば、端末は、乱数を発生してその乱数をICカード1に送信するとともに（ステップT6）、その乱数を自身の暗号化キーを用いて暗号化する（ステップT7）。

【0107】

ICカード1は、相手端末から送信されてきた乱数を受信すると（ステップC5）、自身の暗号化キーを読み出し（ステップC6）、その暗号化キーを用いて受信された乱数を暗号化する（ステップC7）。ICカード1は、さらに、その暗号化された乱数を相手端末に送信して（ステップC8）、相手端末からの応答を待つ。



## 【0108】

端末は、ICカード1から暗号化された乱数を受信すると（ステップT8）、自身で暗号化した乱数とICカード1で暗号化された乱数とを比較する（ステップT9）。そして、2つの暗号化された乱数が一致した場合には（ステップT10）、端末側の認証でICカード1が適合するものであるという判断が下される。したがって、端末はICカード1に対して適合応答する（ステップT11）。一方、2つの暗号化された乱数が不一致であった場合には（ステップT10）、端末側の認証でICカード1が不適合するものであるから、この取引きはないものとして処理が終了する。

## 【0109】

端末からICカード1に適合応答が行われた場合には、ICカード1は、その適合応答を受け付けて（ステップC9）、今度は自ICカード1側で乱数を発生する。ICカード1は、この乱数を相手端末に送信する（ステップC10）。ICカード1は、この乱数発生とともに、自身の暗号化キーを用いて乱数を暗号化する（ステップC11）。

## 【0110】

端末は、ICカード1から送信されてきた乱数を受信すると（ステップT12）、自身の暗号化キーを読み出し（ステップT13）、その暗号化キーを用いて受信された乱数を暗号化してからICカード1に送信する（ステップT14）。そして、端末は、ICカード1からの応答を待つ。

## 【0111】

ICカード1は、相手端末から暗号化された乱数を受信すると（ステップC12）、自身で暗号化した乱数と相手端末で暗号化された乱数とを比較する（ステップC13）。そして、2つの暗号化された乱数が一致した場合には（ステップC14）、ICカード1側の認証で相手端末が適合するものであるという判断が下される。したがって、ICカード1は相手端末に対して適合応答する（ステップC15）。一方、2つの暗号化された乱数が不一致であった場合には（ステップC14）、ICカード1側の認証で相手端末が不適合するものであるから、この取引きはないものとして処理が終了する。

【0112】

なお、端末は、ICカード1から適合応答されると（ステップT15）、取引を開始するが、不適合であれば、ICカード1との取引を中止する。

【0113】

このように、前処理では、端末とICカード1との両方が相手の適合性を認めない限り、取引を実施しないため、高いセキュリティを保持した上での電子財布システムを実現することができる。

【0114】

つぎに、利用装置4について具体例を用いて説明する。図21は実施の形態において利用装置の一例である一般取引機の構成例を示すブロック図である。図21に示した一般取引機は、パチンコ店に設置され、ICカード1を用いたパチンコ玉の排出制御や現金交換等を実施する。

【0115】

図21に示した一般取引機は、ICカードリーダー/ライタ401、表示器402、テンキー403、バーコードリーダー等の機器404、レシートプリンタ405、CPU406、メモリ407、店舗用カード処理器408等により構成される。なお、パチンコ排出や現金交換などの処理そのものは、一般取引機に接続される他の装置（不図示）によって行われるものとする。

【0116】

ICカードリーダー/ライタ401は、ICカード1を装着してICカード1に記憶されたデータを読み出したり書き込む。表示器402は、取引時の情報を可視表示する。テンキー403は、ICカード1による支払い額などを入力するための数字キーである。バーコードリーダー等の機器404は、バーコードが記録されたシートからバーコードデータを読み取る機器である。レシートプリンタ405は、パチンコ玉変換や現金変換等のサービスの結果などを記録する。CPU406は、この一般取引機全体の処理を制御する。メモリ407は、CPU406が動作するためのプログラムを格納したROMおよびCPU406のワークエリアとして使用されるRAMよりなる。店舗用カード処理器408は、店舗独自のカードを処理する機器である。

【0117】

さらに他の例について説明する。図22は実施の形態において利用装置の一例である一般取引電話機の構成例を示すブロック図である。

【0118】

図22に示した一般取引電話機は、ICカードリーダー/ライタ501、表示器502、電話機等サービス/度数制御の機器503、レシートプリンタ504、CPU505、メモリ506、店舗用カード処理器507等により構成される。

【0119】

ICカードリーダー/ライタ501は、ICカード1を装着してICカード1に記憶されたデータを読み出したり書き込む。表示器502は、取引時の情報を可視表示する。電話機等サービス/度数制御の機器503は、図示せぬ電話回線に接続され、電話機能を果たす際に時間および通話距離等に応じて課金する度を制御する。レシートプリンタ504は、電話サービスの結果などを記録する。CPU505は、この一般取引電話機全体の処理を制御する。メモリ506は、CPU505が動作するためのプログラムを格納したROMおよびCPU505のワークエリアとして使用されるRAMよりなる。店舗用カード処理器507は、店舗独自のカードを処理する機器である。

【0120】

つぎに、利用装置4の動作について説明する。まず、一般取引機の動作について説明する。図23、図24および図25は図21に示した一般取引機とICカード1間の取引動作を説明するフローチャートである。この一般取引機は領域IDをもたず、機械IDに従って処理を実行する。

【0121】

図21に示した一般取引機は、まず、前処理を実行する（ステップT101）。この前処理は前述した端末の動作と同様に実施される（図19および図20参照）。一方、ICカード1においても、前処理が実行され（ステップC101）、その処理内容は前述した図19および図20に従うものである。

【0122】

一般取引機が前処理を終了すると、続いて自身の機械IDを読み出される（ス

テップT102)。このとき、一般取引機の表示器402に支払い要求額の入力を要請する表示画面が形成される。この段階では、支払い要求額の入力が可能となり、以降でその支払い要求額が入力された場合には、その支払い要求額は一時メモリ407に格納される。そして、機械IDが支払いコマンドとともにICカード1に送信された後（ステップT103）、一般取引機は、ICカード1から送られてくる第2財布の金額の受信待ちとなる（ステップT104）。

#### 【0123】

ICカード1は、IDおよび支払いコマンドを受信すると（ステップC102）、その支払いコマンドに領域IDが含まれているか否かを判断する（ステップC103）。もし支払いコマンドに領域IDが含まれていた場合には（ステップC103）、第2ディレクトリD2から第2財布アドレスが読み取られ（ステップC104）、一方、含まれていなかった場合には（ステップC103）、この取引は終了する。

#### 【0124】

処理がステップC105に移行した場合には、受信された機械IDが第2ディレクトリD2の機械IDと一致するか否か判断される。もし一致する場合には、続くステップC106において、第2財布アドレスに従って第2財布エリア106Bから残高が読み出されるとともに、その残高が一般取引機に出力される。

#### 【0125】

一般取引機は、ICカード1から第2財布の残高を受信すると（ステップT105）、その受信額を表示器402に表示する（ステップT106）。そして、この段階ですでにテンキー403の操作による支払い要求額の入力がなされていれば（ステップT107）、処理はステップT111に移行する。ステップS111では、メモリ407に格納された支払い要求額が読み出され、ICカード1に送信される。その後、処理はステップT112に移行する。

#### 【0126】

一方、支払い要求額が未入力であれば（ステップT107）、処理は一定時間の入力待ちとなり（ステップT108）、その支払い要求額はテンキー403により入力された段階で（ステップT109）、そのままICカード1に送信され

る（ステップT110）。その後、処理はステップT112に移行する。

【0127】

ICカード1は、一般取引機よりすでに支払いコマンドを受信しており（ステップC107）、さらに支払い要求額を受信する（ステップC108）。この場合、ICカード1は、第2財布の残高から受信された支払い要求額を差し引いてその結果得られた金額をワークエリアW1に格納する（ステップC109）。

【0128】

そして、ワークエリアW1の格納額がゼロもしくはプラスであれば（ステップC110）、支払い可としてその支払い可の情報と支払い額とが一般取引機に通知される（ステップC111）。この後、処理は受け取りコードの待ち状態となる。一方、ワークエリアW1の格納額がマイナスであれば（ステップC110）、この取引きはなかったものとして処理は終了する。

【0129】

一般取引機は、ICカード1より支払い可としての支払い額を受信すると（ステップT112）、その支払い額を表示器402に利用者が確認できるように表示する（ステップT113）。そして、処理はテンキー403に設けられた確認キーの操作による確認待ち状態となる（ステップT114）。利用者が確認キーを操作した場合には、その確認操作が受け付けられ（ステップT114）、ICカード1に対して確認応答が送信され（ステップT115）、さらに支払い額の受信完了を示す受け付けコードが送信される（ステップT116）。

【0130】

ICカード1は、確認応答の受信を一定時間内に受け付けると（ステップC112）、さらに受け取りコードを受信する（ステップC114）。なお、一定時間内に確認応答が受け付けられなかった場合には、この取引きはなかったものとしてワークエリアW1はクリアされ（ステップC113）、処理が終了する。

【0131】

ステップC114において受け取りコードが受信された後、処理はステップC115に移行して、ワークエリアW1の格納額を第2財布エリア106Bに格納する。これによりサービスと交換に支払う金額分が第2財布から取り出されるこ

となる。そして、第3財布エリア106Cには、この取引の履歴（日付など）が格納され（ステップC116）、最後に取り引完了署名コードが一般取引機に送信される（ステップC117）。

#### 【0132】

一般取引機は、ICカード1から取引完了署名コードを受信すると、自己取引履歴の作成および残高更新を行って（ステップT117）、サービス処理（パチンコ玉排出制御、現金交換等）を実行する（ステップT118）。最後に、ICカード1がICカードリーダー/ライター401から返却される（ステップT119）。

#### 【0133】

続いて、一般取引電話機の動作について説明する。図26、図27および図28は図22に示した一般取引電話機とICカード1間の取引動作を説明するフローチャートである。

#### 【0134】

図22に示した一般取引電話機は、まず、前処理を実行する（ステップT201）。この前処理は前述した端末の動作と同様に実施される（図19および図20参照）。一方、ICカード1においても、前処理が実行され（ステップC201）、その処理内容は前述した図19および図20に従うものである。

#### 【0135】

一般取引電話機が前処理を終了すると、続いて自身の機械IDが読み出される（ステップT202）。このとき、一般取引電話機の表示器502に支払い要求額の入力を要請する表示画面が形成される。この段階では、支払い要求額の入力が可能となり、以降でその支払い要求額が入力された場合には、その支払い要求額は一時メモリ506に格納される。そして、機械IDが支払いコマンドとともにICカード1に送信された後（ステップT203）、一般取引電話機は、ICカード1から送られてくる第2財布の金額の受信待ちとなる（ステップT204）。

#### 【0136】

ICカード1は、IDおよび支払いコマンドを受信すると（ステップC202

）、その支払いコマンドに領域IDが含まれているか否かを判断する（ステップC203）。もし支払いコマンドに領域IDが含まれていた場合には（ステップC203）、第2ディレクトリD2から第2財布アドレスが読み取られ（ステップC204）、一方、含まれていなかった場合には（ステップC203）、この取引は終了する。

## 【0137】

処理がステップC205に移行した場合には、受信された機械IDが第2ディレクトリD2の機械IDと一致するか否か判断される。もし一致する場合には、続くステップC206において、第2財布アドレスに従って第2財布エリア106Bから残高が読み出されるとともに、その残高が一般取引電話機に出力される。

## 【0138】

一般取引電話機は、ICカード1から第2財布の残高を受信すると（ステップT205）、その受信額を表示器502に表示する（ステップT206）。この後、一般取引電話機では、電話機能のサービスが開始される。

## 【0139】

一般取引電話機は、サービス開始後、通話に応じて単位サービス額を検知するとともに度数制御に従う金額カウンタを更新する（ステップT207）。そして、第2財布の残金すなわち表示器502に表示されている表示額（受信額）から刻々更新される金額カウンタの値が差し引かれ、その結果得られる使用可能金額がゼロに達するまで（ステップT208）、もしくは、サービスの終了が検知されるまでは（ステップT210）、ステップT207における金額カウンタの更新、ステップT208における使用可能金額の算出およびステップT209における使用可能金額の表示（表示器502の表示ワークエリアへの表示）が実行される。

## 【0140】

そして、使用可能金額がゼロとなった場合（ステップT208）、もしくはサービスの終了が検知された場合（ステップT210）、処理はステップT211に移行して、支払い額の請求が受信されるのを待つ（ステップT211）。この

ようにして支払額の請求が受信されると（ステップT211）、金額カウンタの値が読み出され、その値が支払い要求額としてICカード1に送信される（ステップT212）。

【0141】

ICカード1は、一般取引電話機よりすでに支払いコマンドを受信しており（ステップC207）、さらに支払い要求額を受信する（ステップC208）。この場合、ICカード1は、第2財布の残高から受信された支払い要求額を差し引いてその結果得られた金額をワークエリアW1に格納する（ステップC209）。

【0142】

そして、ワークエリアW1の格納額がゼロもしくはプラスであれば（ステップC210）、支払い可としてその支払い可の情報と支払い額とが一般取引電話機に通知される（ステップC211）。この後、処理は受け取りコードの待ち状態となる。一方、ワークエリアW1の格納額がマイナスであれば（ステップC210）、この取引きはなかったものとして処理は終了する。

【0143】

一般取引電話機は、ICカード1より支払い可としての支払い額を受信すると（ステップT213）、その支払い額を表示器502に利用者が確認できるように表示する（ステップT214）。そして、処理は電話機等サービス/度数制御の機器503に設けられた確認キーの操作による確認待ち状態となる（ステップT215）。利用者が確認キーを操作した場合には、その確認操作が受け付けられ（ステップT215）、ICカード1に対して確認応答が送信され（ステップT216）、さらに支払い額の受信完了を示す受け付けコードが送信される（ステップT217）。

【0144】

ICカード1は、確認応答の受信を一定時間内に受け付けると（ステップC212）、さらに受け取りコードを受信する（ステップC214）。なお、一定時間内に確認応答が受け付けられなかった場合には、この取引きはなかったものとしてワークエリアW1はクリアされ（ステップC213）、処理が終了する。



## 【0145】

ステップC214において受け取りコードが受信された後、処理はステップC215に移行して、ワークエリアW1の格納額を第2財布エリア106Bに格納する。これによりサービスと交換に支払う金額分が第2財布から取り出されることになる。そして、第3財布エリア106Cには、この取引の履歴（日付など）が格納され（ステップC216）、最後に取り引完了署名コードが一般取引機に送信される（ステップC217）。

## 【0146】

一般取引電話機は、ICカード1から取引完了署名コードを受信すると、自己取引履歴の作成、残高更新およびレシート印刷を行い（ステップT218）、最後に、ICカード1をICカードリーダー/ライター501から返却する（ステップT219）。

## 【0147】

つぎに、引出装置2の動作について説明する。図29～図32は実施の形態において引出装置とICカード間の取引動作を説明するフローチャートであり、図33は実施の形態において引出装置による取引動作時の表示画面の一例を示す図である。

## 【0148】

図29～図32に示したフローチャートは、引出装置2が預金引出機の例を示している。引出装置2は、まず、ICカード1との引出し取引を行うため、表示画面に取引金額入力、暗証番号、カード挿入指示を提示する（ステップT301）。この提示の後、引出装置2は前処理に入る（ステップT302）。これに伴ってICカード1も前処理を実行する（ステップC301）。

## 【0149】

続いて、引出装置2は、金額入力および暗証番号入力を経た後（ステップT303）、支払いコマンドに機械IDおよび領域ID（第1財布の指定）を含めて送信する（ステップT304）。

## 【0150】

ICカード1は、引出装置2より支払いコマンドを受信すると（ステップC3

02)、その受信された支払いコマンドに領域IDが含まれることから(ステップC303)、領域IDの領域を読み取る(ステップC304)。

【0151】

ICカード1は、支払いコマンド中の機械IDを読み出してその機械IDと第1ディレクトリD1の機械IDと比較する。そのとき、両機械IDが一致すれば(ステップC305)、さらにその機械IDのアクセス権と受信アクセスとの対応を確認する(ステップC306)。なお、機械IDの不一致が確認されると(ステップC305)、この引出し取引はなかったものとして無効にされる。

【0152】

ステップC306において対応関係が確認されると、処理はさらにステップC307に移行する。ステップC307では、ステップC304で読み取られた領域が第1財布であれば、処理はステップC308に移行し、そうでなければ、処理は他モードを実行する。

【0153】

処理がステップC308に移行すると、引出装置2の要求内容を判別する。この場合には、引出装置2が支払いコマンドを送信していることから、要求は支払いと判別される。したがって、ここでは、支払いについてのみ図示(図29、図30および図31参照)およびその説明を詳述し、他の転送、カード預金などは、前述したICカード1の動作に従うものとする。

【0154】

さて、支払い要求の場合には、すでに説明した図12および図13の支払い処理が開始される。この支払い処理では、まず、引出装置2に対して暗証番号および要求額が要請される(ステップC309)。

【0155】

引出装置2は、ICカード1より暗証番号と支払い額との要請を受け付けると、その両情報が入力済みであるか判断する(ステップT305)。この場合、ステップT303において両情報はすでに入力済みであることから、処理はつぎのステップT306に移行する。ステップT306において両情報すなわち暗証番号と支払い額とが暗号化され、続くステップT307においてこれら暗号化情報

はICカード1に送信される。

【0156】

ICカード1は、その後、暗証番号および支払い要求額を受信すると（ステップC310）、まず暗証番号を復号する（ステップC311）。このようにして暗証番号が復号されると、続くステップC312において、第1ディレクトリD1に格納されている暗証番号が読み出され、その暗証番号が復号される。

【0157】

さらに、この復号されたICカード1自身の暗証番号と取引装置2から受け取って復号した暗証番号との照合が行われ（ステップC313）、両暗証番号が一致した場合には（ステップC314）、認証をパスできたものとして処理はステップC315に移行する。一方、認証をパスできなかった場合には、この支払い取引きはなかったものとして無効にされる。

【0158】

さらに、ICカード1では、第1財布エリア106Aおよび第2財布エリア106Bの各残高が暗号化して引出装置2に送信される（ステップC315）。これにより、引出装置2は、ICカード1から第1財布、第2財布の各残高を受信すると（ステップT308）、残高表示を行って利用者に第1財布と第2財布の残り金額を提示する（ステップT309）。その後、引出装置2はICカード1からの支払い可の通知を待つ（ステップT310）。

【0159】

ICカード1では、受信された支払い要求額が復号される（ステップC316）。その後、第1財布エリア106Aに格納された残高から復号された支払い要求額が差し引かれ、その金額がワークエリアW2に格納される（ステップC317）。

【0160】

そして、ワークエリアW2に格納された金額がゼロもしくはプラスであった場合には（ステップC318）、支払い可となることからその支払い可の情報、第1財布の残高およびワークエリアW2に格納された金額がそれぞれ暗号化される（ステップC322）。このようにして暗号化された各情報は暗号化情報として

引出装置2に送信される（ステップC323）。一方、ワークエリアW2に格納された金額がマイナスであった場合には（ステップC318）、処理はステップC319に移行して図14に示した追加取引を実行する。

#### 【0161】

すなわち、ICカード1はさらに第2財布エリア106Bから残高を読み取り（ステップC319）、その金額をワークエリアW2の格納額に加算してその合計をワークエリアW2の格納額とする（ステップC320）。この後に、再度ワークエリアW2の格納額がゼロもしくはプラスに転じていれば、ICカード1は上述したステップC322およびステップC323において支払い可、第1財布の残高およびワークエリアW2の格納額の暗号化および送信を実行する。

#### 【0162】

引出装置2は、ICカード1から暗号化情報を受信して支払い可を確認すると（ステップT310）、図33に示したように、ワークエリアW2の金額から支払い前後の残高確認表示を行う（ステップT311）。

#### 【0163】

この残高確認表示では、第1財布、第2財布それぞれの支払い前と支払い後の金額（一例として円表示）が表示され、さらに支払い額、確認操作のためのアイコン「確認」および取り消し操作のためのアイコン「取消」が表示される。これらの操作は図示せぬキー操作パネルによって行われる。図33の例では、第1財布の支払い前後の金額はそれぞれa円、A円となり、第2財布の支払い前後の金額はそれぞれb円、B円となる。さらに、支払い額はC円となる。

#### 【0164】

そして、引出装置2は利用者による確認操作を待ち（ステップT312）、その確認操作を受け付けると同時にICカード1に対して確認応答の送信（ステップT313）および受け取りコードの送信を行う（ステップT314）。ここで、受け取りコードとは、確かにICカード1より支払いを受けたということを証明するものである。

#### 【0165】

ICカード1において、ステップC323の暗号化送信の後、引出装置2から

一定時間内に応答受信がない場合には（ステップC324）、処理はステップC325に移行して、この支払い取引はなかったものにするため、ワークエリアW2はクリアされる。一方、ステップC324において応答受信が確認された場合には、その応答受信によって受信されたデータが受け取りコードか否か判断される（ステップC326）。

【0166】

受信データが受け取りコードであった場合には、支払い取引が成立したものとして、ワークエリアW2の暗号化された金額が第1財布エリア106Aに格納される（ステップC327）。このようにして、第1財布エリア106Aは、支払い要求金額に従って残高が更新される。

【0167】

さらに、第3財布エリア106Cには、上述した転送取引の日付などの情報が履歴として格納される（ステップC328）。最後に、取引装置2に対してICカード1内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップC329）。

【0168】

引出装置2は、ICカード1から取引完了署名コードを受け取ると、自己取引履歴を作成して自己のICカードに記録するとともに、残高更新およびレシート印刷を行った後に処理を終了する（ステップT315）。

【0169】

つぎに、引出装置2の応用例を用いて説明する。図34は実施の形態において引出装置の一例であるATM（Automatic Teller Machine）機の構成例を示すブロック図である。

【0170】

図34に示したATM機は、CRT／タッチパネル601、表示制御部602、入力検知部603、ICカードリーダー／ライター604、インタフェース605、キャッシュカウンタ／預金機構606、機構制御部607、回線制御部608、暗号化／復号化ボード609、CPU610、メモリ611、外部メモリ612、銀行用ICカードリーダー613などにより構成される。

## 【0171】

CRT/タッチパネル601は、表示画面をタッチしてデータや各種の操作を入力する。表示制御部602は、CRT/タッチパネル601のCRT表示を制御し、入力検知部603は、CRT/タッチパネル601のタッチ入力を検知する。ICカードリーダー/ライター604は、ICカード1を装着してデータの読み出しや書き込みを行う。インタフェース605は、ICカード1とATM機内部とのインタフェースを司る。

## 【0172】

キャッシュカウンタ/預金機構606は、金額をカウントして支払うキャッシュカウンタと金額をカウントして口座に入金する制御機構である。機構制御部607は、キャッシュカウンタ/預金機構606を制御する。回線制御部608は、回線を介してセンタシステム3のホストコンピュータ31と通信を制御する。暗号化/復号化ボード609は、取引き時におけるデータの暗号化および復号化を行う。

## 【0173】

CPU610は、装置全体を制御する。メモリ611はCPU610が動作するためのプログラムを格納したROMおよびCPU610のワークエリアとして使用するRAMにより構成される。外部メモリ612は、ハードディスクなどの大容量メモリである。銀行用ICカードリーダー613は、オンラインバンキングの手続きを行うための通常の銀行カードを装着して認証情報を読み出す。

## 【0174】

つぎに、ATM機の動作について説明する。図35～図37は図34に示したATM機とICカード間の取引動作を説明するフローチャートであり、図38および図39は実施の形態においてATM機による取引動作時の表示画面の一例を示す図である。

## 【0175】

ATM機は、まず、ICカード1との引出し取引を行うため、図38(a)に示したように、CRT/タッチパネル601に、カード挿入指示、暗証番号入力、モード入力を提示した初期画面を形成する(ステップT401)。この初期

画面形成後、ATM機は前処理に入る（ステップT402）。これに伴ってICカード1も前処理を実行する（ステップC401）。

## 【0176】

続いて、ATM機は、カード挿入指示を消去するなどして第2画面を表示する（ステップT403）。その後、CRT／タッチパネル601へのタッチ操作によりモード（支払い、預金（カード預金）、振込、残高照会）指定が行われると（ステップT404）、その指定モードがいずれであるのか判断される（ステップT405）。ここでは、支払いモードについての例を挙げる。したがって、支払いモード以外のモードが指定された場合には、他のモード処理として図示および説明を省略する。

## 【0177】

なお、他のモードとして、預金モードが指定された場合には、図38（c）に示した預金モード画面のように、さらに細かいモードとして現金からICカードへのモードと現金を口座へ移すモードとが用意される。また、振込モードが指定された場合には、図38（d）に示した振込モード画面のように、さらに細かいモードとしてICカードから振込先へのモードと口座から振込先へのモードとが用意される。また、残高照会モードが指定された場合には、図38（e）に示したように、さらに細かい指定として口座預金残高、口座とICカードとの両残高、ICカード残高の3つが用意される。

## 【0178】

さて、支払いモードが指定された場合には（ステップT405）、図38（b）に示したように、CRT／タッチパネル601に、支払いモード画面が形成される（ステップT406）。そして、この支払いモード画面についても、さらに細かくモード指定が行われる。

## 【0179】

すなわち、支払いモード画面には、口座からICカードへ、口座から現金へ、ICカードからICカードへ、ICカードから現金へ、口座からICカードおよび現金へ、ICカードからICカードおよび現金への6種類のモードが用意される（図38（b）～（e）では、ICカードを省略してカードで示している）。

利用者はこれら6種類のモードから所要のモードをタッチ操作により指定する。ここでは、口座からICカード1へのモードが指定された場合を例に挙げ、その他のモードについては他のモード処理として図示および説明を省略する。

## 【0180】

口座／カードモードが指定された場合には、CRT／タッチパネル601に図39(a)に示した金額指定画面が表示され、その金額指定画面に対する操作および画面編集が行われる(ステップT409)。図39(a)に示した金額指定画面は、A1(仮の一方)からA2(仮の他方)へ引き落とす金額を入力する旨の指示、金額を入力するための数字キー、金額の単位(一例として“万円”, “千円”)を入力するためのキー、金額入力後の確認キー、このモードを取り消すための取消キーが表示される。いずれの表示も、タッチ入力が可能である。

## 【0181】

ここで、指定されたモードが口座／カードモードであることから、A1には“口座”が設定され、A2には“カード”(ICカード1の意味)が設定される(ステップT410)。そして、図39(a)の金額指定画面において処理は金額の指定待ちとなる(ステップT411)。その後、金額指定があると(ステップT411)、処理はさらに暗証番号の入力待ちとなる(ステップT412)。

## 【0182】

ATM機は、このようにして金額指定および暗証番号入力を経た後(ステップT411およびステップT412)、更新コマンドに暗証番号、支払い要求額(金額指定された額)、機械ID、領域ID(ここでは第1財布の指定)を含めた暗号化送信を行う(ステップT413)。なお、更新コマンドとしたのは、A1からA2への金額の移動でA1とA2の残高が更新されるためである。ただし、この更新コマンドは、ステップT405で指定したモードを特定する内容となる。

## 【0183】

ICカード1は、ATM機より支払いコマンドを受信すると(ステップC402)、その受信された更新コマンドに領域IDが含まれることから(ステップC403)、領域IDの領域を読み取る(ステップC404)。



## 【0184】

ICカード1は、更新コマンド中の機械IDを読み出してその機械IDと第1ディレクトリD1の機械IDと比較する。そのとき、両機械IDが一致すれば（ステップC405）、さらにその機械IDのアクセス権と受信アクセスとの対応を確認する（ステップC406）。なお、機械IDの不一致が確認されると（ステップC405）、この引出し取引はなかったものとして無効にされる。

## 【0185】

ステップC406において対応関係が確認されると、処理はさらにステップC407に移行する。ステップC407では、ステップC404で読み取られた領域が第1財布であれば、処理はステップC408に移行し、そうでなければ、処理はステップC412に移行してさらにモード指定が支払いモードか否かを確認する。

## 【0186】

ICカード1において、処理がステップC408に移行した場合には、領域IDが第3財布すなわちセンタ口座情報を指定しているか否かを判断する。上述の流れでは、第1財布のため、この場合にもこの取引はなかったものとして処理は終了する。なお、第3財布の指定であった場合には、処理はさらにステップC409に移行してセンタ口座情報のアクセス権を確認する。そこで、ATM機が読み出しできる機械であった場合には（ステップC409）、続くステップC410において口座番号が読み出され、その口座番号がATM機に出力される（ステップC411）。その後、この取引は終了する。

## 【0187】

ステップC407において領域IDが第1財布を指定していた場合には、処理はステップC412に移行するので、そこで要求内容が判別される。上述の流れでは、要求は支払いと判別される。したがって、ここでは、支払いについてのみ図示（図29、図30および図31参照）およびその説明を詳述し、他の転送、カード預金などは、前述したICカード1の動作に従うものとする。

## 【0188】

さて、支払い要求の場合には、すでに説明した図12および図13の支払い処

理が開始される。ICカード1は、すでにステップC401において暗証番号および支払い要求額を受信している。したがって、まず、暗証番号が復号され（ステップC413）、続くステップC414において、第1ディレクトリD1に格納されている暗証番号が読み出され、その暗証番号が復号される。

【0189】

さらに、この復号されたICカード1自身の暗証番号とATM機から受け取って復号した暗証番号との照合が行われ（ステップC415）、両暗証番号が一致した場合には（ステップC416）、認証をパスできたものとして処理はステップC417に移行する。一方、認証をパスできなかった場合には、この支払い取引はなかったものとして無効にされる。

【0190】

さらに、ICカード1は、第1財布エリア106Aおよび第2財布エリア106Bの各残高を暗号化してからATM機に送信する（ステップC417）。

【0191】

ATM機は、ステップT413による暗号化送信の後、ICカード1からの第1財布、第2財布の各残高（暗号化情報）の受信待ちとなる（ステップT414）。その待ち時間が一定時間を経過すると、処理は強制的にカード返却に移行して終了する。

【0192】

ATM機において、一定時間内にICカード1から第1財布、第2財布の各残高（暗号化情報）が受信されると（ステップT414）、まず、暗証番号、口座情報、引き落とし額（支払い額）がセンタシステム3に送信される（ステップT416）。なお、口座情報については、上述したステップC408～ステップC411をICカード1に実行させることで取得することができる。続いて、その受信された各残高は図39（b）に示したように、CRT/タッチパネル601に表示される（ステップT417）。その後、ATM機はセンタシステム3からの支払い可の通知を待つ（ステップT419）。

【0193】

ICカード1は、ステップC417において暗号化情報を送信した後、すでに

受信された支払い要求額を復号する（ステップC418）。その後、第1財布エリア106Aに格納された残高にその復号された支払い要求額が加算され、その金額がワークエリアW2に格納される（ステップC419）。そして、処理はATM機からの確認コードの受信待ちとなる（ステップC420）。

【0194】

ATM機は、センタシステム3より支払い可の通知を受け取ると（ステップT418）、利用者による確認操作に従って（ステップT419）、ICカード1に対して確認コードを送信する（ステップT420）。この後に、ICカード1より取引完了署名コードが受信されると、履歴などの処理を経てATM機側の処理が終了する。

【0195】

ICカード1において、ATM機から確認コードが受信された場合には（ステップC420）、支払い取引が成立したものとして、ワークエリアW2の暗号化された金額が第1財布エリア106Aに格納される（ステップC421）。このようにして、第1財布エリア106Aは、口座からICカードへの支払い要求金額に従って残高が更新される。

【0196】

さらに、第3財布エリア106Cには、上述した転送取引の日付などの情報が履歴として格納される（ステップC422）。最後に、ATM機に対してICカード1内の処理が完了したことを通知するため、取引完了署名コードが相手端末に送信される（ステップC423）。

【0197】

さて、上述した処理は、口座からICカード1への支払いモードを例に挙げているが、その他に、例えば、口座からICカードおよび現金へ、もしくは、ICカードからICカードおよび現金への支払いであれば、図39（c）の如く表示画面が形成される。この場合には、支払先となる財布（例えば第2財布でも可）や現金について、それぞれ引き落としたい金額を指定することができる。

【0198】

また、図39（b）には、財布の残高を表示させるだけであったが、図39（

d) のように、取引完了後の口座残高についても表示するようにしてもよい。

【0199】

以上説明したように、この実施の形態によれば、二重財布（ＩＣカード）としての特性が生かされ、セキュリティの低い方の第２財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の第１財布についてはさらにセキュリティを向上させることが可能である。

【0200】

また、利用装置が領域指定せずに支払い処理を要求した場合には、第２財布の預金額を用いて、セキュリティの低い、個人認証を伴わない簡易な利用取引を実現することが可能である。

【0201】

また、ＩＣカード１により、セキュリティの低い第２財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第１財布については個人認証や暗号利用により不正防止を図ることが可能である。

【0202】

また、取引装置とＩＣカードとの取引で、一定時間内に任意のモード指定を受け付けた場合にセンタ口座の利用を許し、受け付けられなかった場合には現金支払いに以降するようにしたので、センタ口座の取引についてはモードによるバリエーションを持たせ、現金での取引についてはその指定操作を省くことで、現金取引の簡略化を実現することが可能である。

【0203】

また、取引装置とＩＣカードとの個人認証を要する取引で、第１財布だけで金額上の取引が成立しなくても第２財布の金額を補填して再度取引を遂行するようにしたので、利用者が取引のための金額を気にすることなく取引を遂行することができ、操作性の向上を図ることが可能である。

【0204】

また、取引装置とＩＣカードとの取引で、個人認証を経た場合にのみ第１財布および第２財布の金額を取引装置に出力し、そうでない場合には第２財布の金額のみ取引装置に出力するようにしたので、照会などで財布の中身を取引装置に

教える程度の取引きであっても、個人認証を通過できなければセキュリティの高い第1財布を開くことを防止することが可能である。

【0205】

以上、この発明を実施の形態により説明したが、この発明の主旨の範囲内で種々の変形が可能であり、これらをこの発明の範囲から排除するものではない。

【0206】

【発明の効果】

以上説明したように、請求項1の発明によれば、二重財布（ICカード）としての特性が生かされ、セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることが可能な二重財布を有する電子財布システムが得られるという効果を奏する。

【0207】

また、請求項1の発明は、請求項2のように、カード状担体の第2不揮発性メモリに第2領域が引出処理のみ許容するプログラムを格納するようにしてもよい。

【0208】

また、請求項1の発明は、請求項3の発明のように、カード状担体に設けた第3領域に当該第3領域へのアクセスを許容する利用装置の識別情報および暗証番号を登録しておき、利用装置から登録されている情報に対応する識別情報および暗証情報が入力された場合に第3領域の加算又は減算を許容するようにしてもよい。

【0209】

また、請求項3の発明は、請求項4の発明のように、カード状担体の第3領域に、加算処理した利用装置を示す識別情報と加算処理した額とを履歴情報として格納するようにしてもよい。

【0210】

また、請求項5の発明によれば、利用装置が領域指定せずに支払い処理を要求した場合には、第2領域の預金額を用いて、セキュリティの低い、個人認証を伴

わない簡易な利用取引を実現することが可能な二重財布を有する電子財布システムが得られるという効果を奏する。

## 【0211】

また、請求項6の発明によれば、セキュリティの低い第2財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第1財布については個人認証により不正防止を図ることが可能な二重財布を有する電子財布システムに適用されるICカードが得られるという効果を奏する。

## 【0212】

また、請求項7の発明によれば、セキュリティの低い第2財布まで暗証照合を行うような手間が省けて使い勝手が向上するとともに、セキュリティの高い第1財布については暗号利用により不正防止機能を一層向上させることが可能な二重財布を有する電子財布システムに適用されるICカードが得られるという効果を奏する。

## 【0213】

また、請求項8によれば、取引装置とICカードとの取引で、一定時間内に任意のモード指定を受け付けた場合にセンタ口座の利用を許し、受け付けられなかった場合には現金支払いに以降するようにしたので、センタ口座の取引についてはモードによるバリエーションを持たせ、現金での取引についてはその指定操作を省くことで、現金取引の簡略化を実現することが可能なICカード取引装置が得られるという効果を奏する。

## 【0214】

また、請求項9の発明によれば、取引装置とICカードとの個人認証を要する取引で、第1財布だけで金額上の取引が成立しなくても第2財布の金額を補填して再度取引を遂行するようにしたので、利用者が取引のための金額を気にすることなく取引を遂行することができ、操作性の向上を図ることが可能なICカード取引装置が得られるという効果を奏する。

## 【0215】

また、請求項10の発明によれば、取引装置とICカードとの取引で、個人認証を経た場合にのみ第1財布および第2財布の金額を取引装置に出力し、そう

でない場合には第2財布の金額のみ取引装置に出力するようにしたので、照会などで財布の中身を取引装置に教える程度の取引であっても、個人認証を通過できなければセキュリティの高い第1財布を開くことを防止することが可能なICカード取引システムに適用されるICカードが得られるという効果を奏する。

【図面の簡単な説明】

【図1】

この発明に係る実施の形態による電子財布システムの一例を示す構成図である。

【図2】

図1に示したICカードを機能的に示すブロック図である。

【図3】

図1に示したICカードをハードウェア的に示すブロック図である。

【図4】

図3に示したICカードのメモリ構成例を示す図である。

【図5】

図1に示した引出装置を機能的に示すブロック図である。

【図6】

図1に示したセンタシステムを概略的に示す構成図である。

【図7】

図1に示した利用装置を機能的に示すブロック図である。

【図8】

この発明に係る実施の形態によるICカードのメイン動作を説明するフローチャートである。

【図9】

この発明に係る実施の形態によるICカードのメイン動作を説明するフローチャートである。

【図10】

図8に示したメイン動作における転送処理を説明するフローチャートである。

【図11】

図8に示したメイン動作における転送処理を説明するフローチャートである。

【図12】

図8に示したメイン動作における支払い処理を説明するフローチャートである。

【図13】

図8に示したメイン動作における支払い処理を説明するフローチャートである。

【図14】

図11に示した支払い処理における追加取引を説明するフローチャートである。

【図15】

図8に示したメイン動作におけるカード預金処理を説明するフローチャートである。

【図16】

図8に示したメイン動作におけるカード預金処理を説明するフローチャートである。

【図17】

この発明に係る実施の形態における復号処理を説明するフローチャートである。

【図18】

この発明に係る実施の形態における暗号化処理を説明するフローチャートである。

【図19】

この発明に係る実施の形態における前処理を説明するフローチャートである。

【図20】

この発明に係る実施の形態における前処理を説明するフローチャートである。

【図21】

この発明に係る実施の形態において利用装置の一例である一般取引機の構成例を示すブロック図である。



【図 2 2】

この発明に係る実施の形態において利用装置の一例である一般取引電話機の構成例を示すブロック図である。

【図 2 3】

図 1 8 に示した一般取引機と I C カード間の取引動作を説明するフローチャートである。

【図 2 4】

図 1 8 に示した一般取引機と I C カード間の取引動作を説明するフローチャートである。

【図 2 5】

図 1 8 に示した一般取引機と I C カード間の取引動作を説明するフローチャートである。

【図 2 6】

図 1 9 に示した一般取引電話機と I C カード間の取引動作を説明するフローチャートである。

【図 2 7】

図 1 9 に示した一般取引電話機と I C カード間の取引動作を説明するフローチャートである。

【図 2 8】

図 1 9 に示した一般取引電話機と I C カード間の取引動作を説明するフローチャートである。

【図 2 9】

この発明に係る実施の形態において引出装置と I C カード間の取引動作を説明するフローチャートである。

【図 3 0】

この発明に係る実施の形態において引出装置と I C カード間の取引動作を説明するフローチャートである。

【図 3 1】

この発明に係る実施の形態において引出装置と I C カード間の取引動作を説明

するフローチャートである。

【図32】

この発明に係る実施の形態において引出装置とICカード間の取引動作を説明するフローチャートである。

【図33】

この発明に係る実施の形態において引出装置による取引動作時の表示画面の一例を示す図である。

【図34】

この発明に係る実施の形態において引出装置の一例であるATM機の構成例を示すブロック図である。

【図35】

図28に示したATM機とICカード間の取引動作を説明するフローチャートである。

【図36】

図28に示したATM機とICカード間の取引動作を説明するフローチャートである。

【図37】

図28に示したATM機とICカード間の取引動作を説明するフローチャートである。

【図38】

この発明に係る実施の形態においてATM機による取引動作時の表示画面の一例を示す図である。

【図39】

この発明に係る実施の形態においてATM機による取引動作時の表示画面の一例を示す図である。

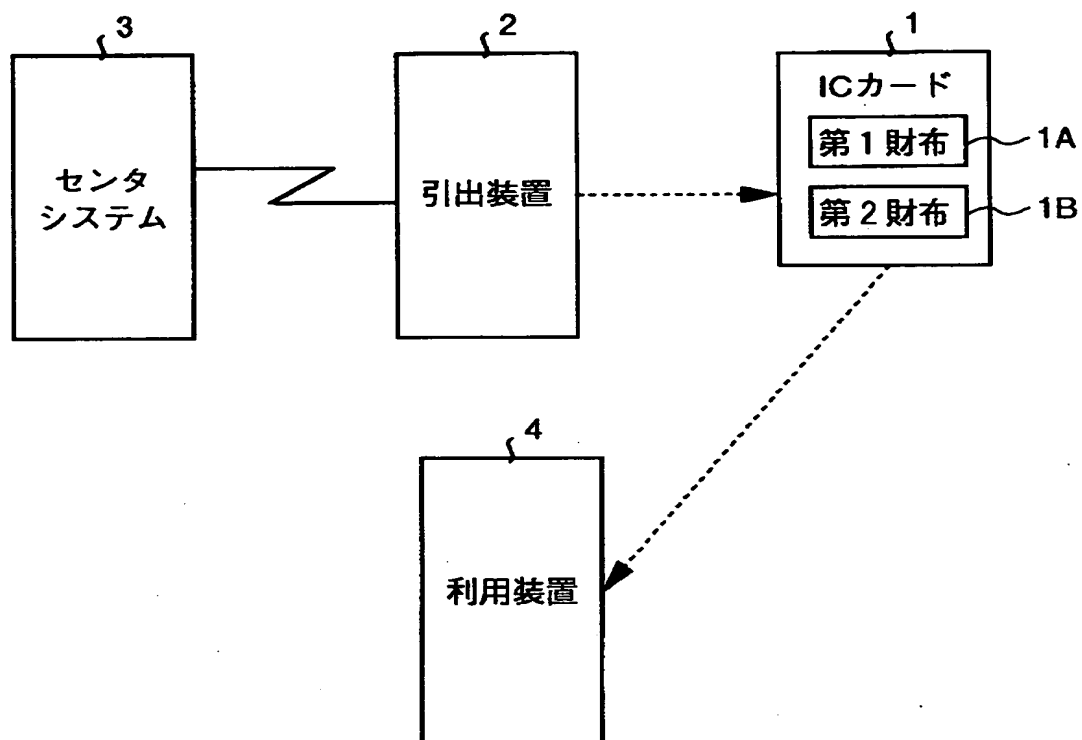
【符号の説明】

- 1 ICカード
- 2 引出装置
- 3 センタシステム

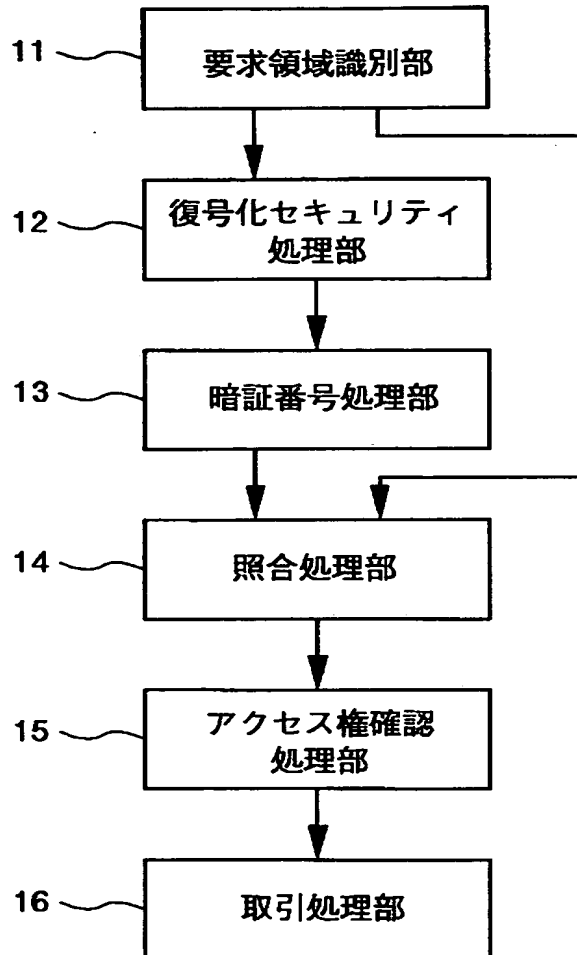
- 4 利用装置
  - 1 1 要求領域識別部
  - 1 2 復号化セキュリティ処理部
  - 1 3 暗証番号処理部
  - 1 4 照合処理部
  - 1 5 アクセス権確認処理部
  - 1 6 取引処理部
  - 2 1 機械IDレジスタ
  - 2 2 認証転送処理部
  - 2 3 暗号化処理部
  - 3 1 ホストコンピュータ
  - 3 2 データベース
  - 4 1 機械IDレジスタ
  - 4 2 転送処理部
  - 4 3 支払い額発生部
  - 4 4 取引処理部
  - 4 5 受信部
  - 4 6 メモリ
- 1 0 3 CPU
- 1 0 4 ROM
- 1 0 5 RAM
- 1 0 6 EEPROM
  - 1 0 6 A 第1財布エリア
  - 1 0 6 B 第2財布エリア
  - 1 0 6 C 第3財布エリア
- 4 0 1, 5 0 1, 6 0 4 ICカードリーダー/ライター
- 4 0 6, 5 0 5, 5 1 0 CPU
- 4 0 7, 5 0 6, 6 1 1 メモリ

【書類名】 図面

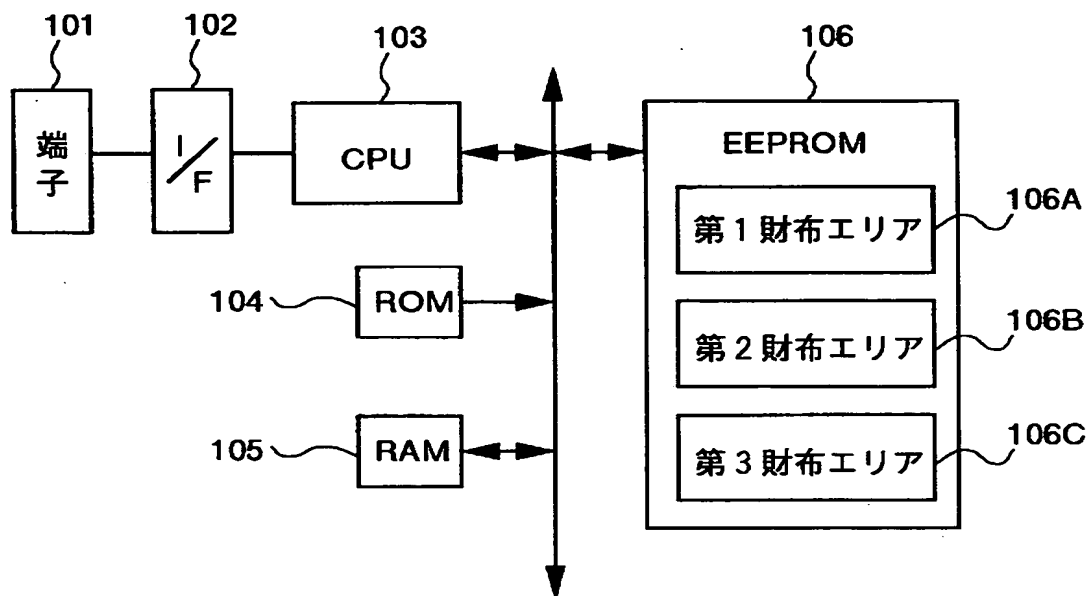
【図1】



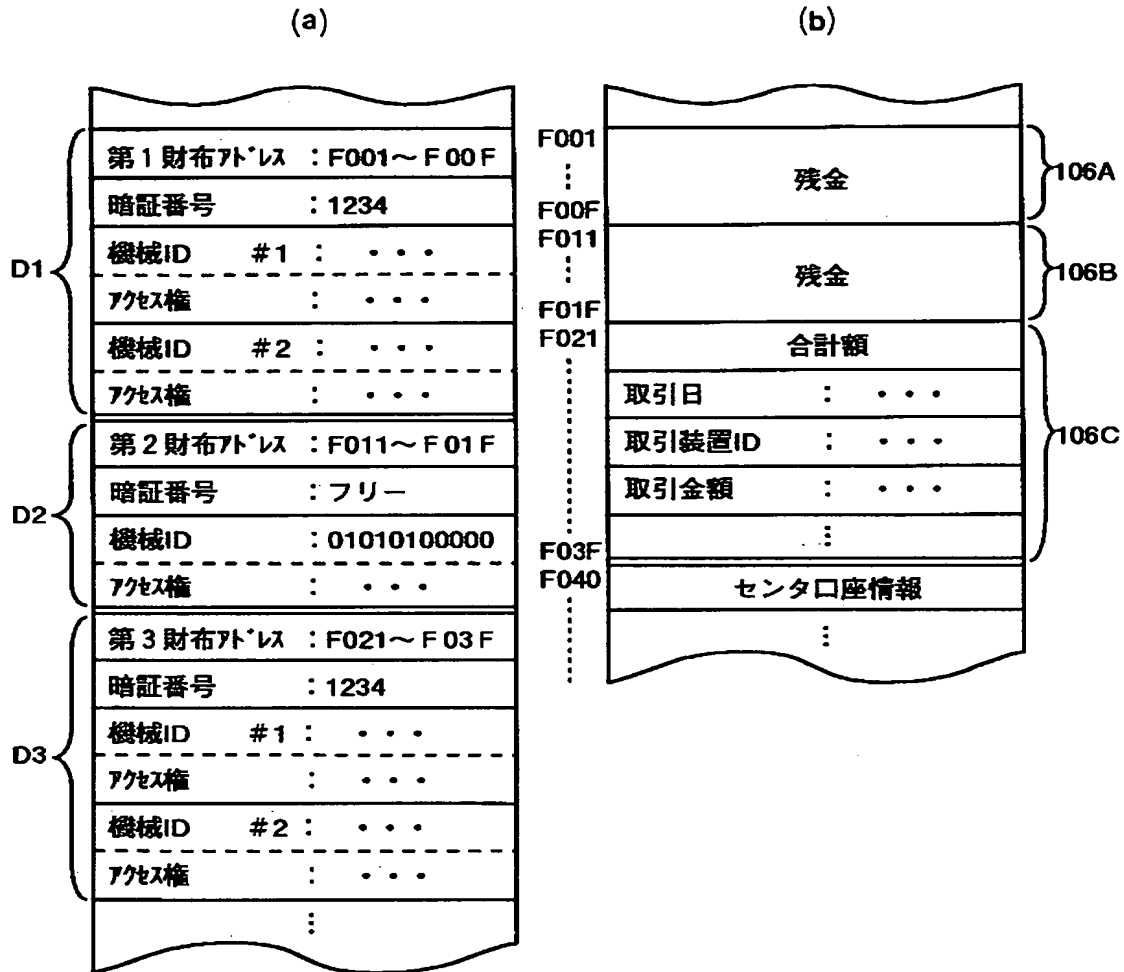
【図2】



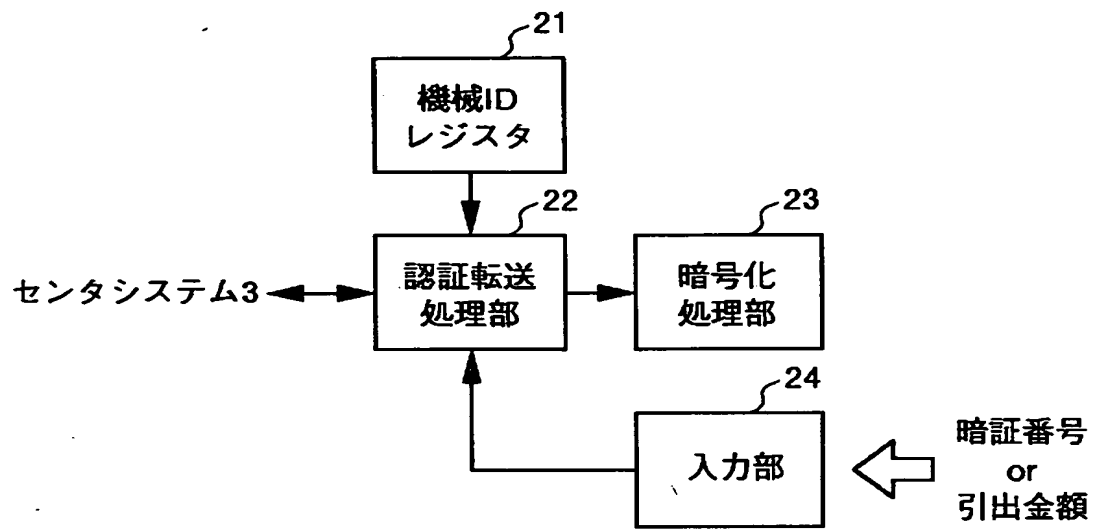
【図3】



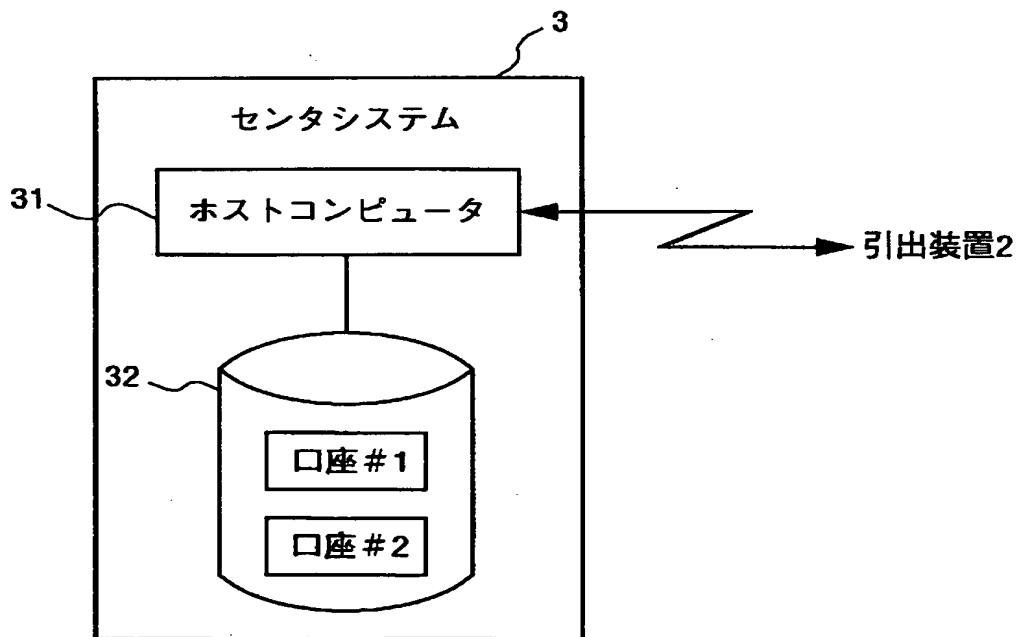
【図4】



【図5】

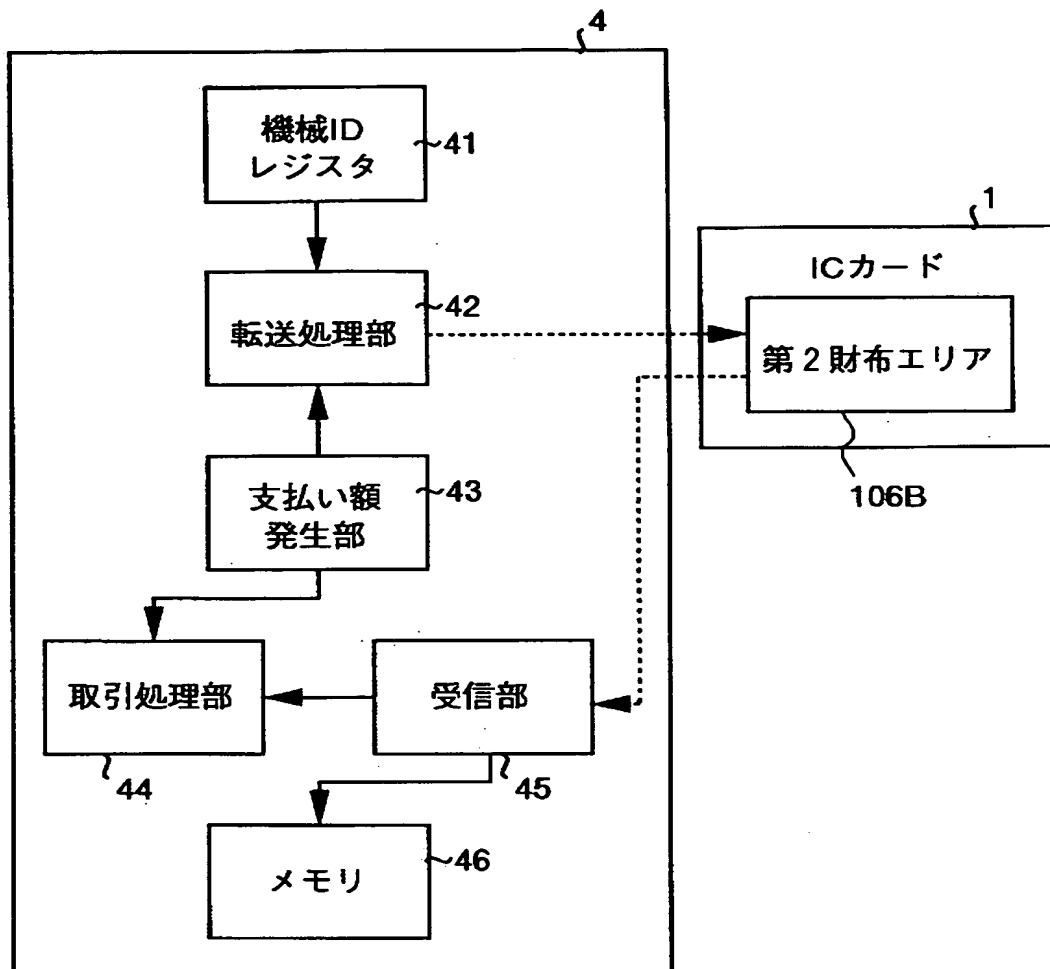


【図6】

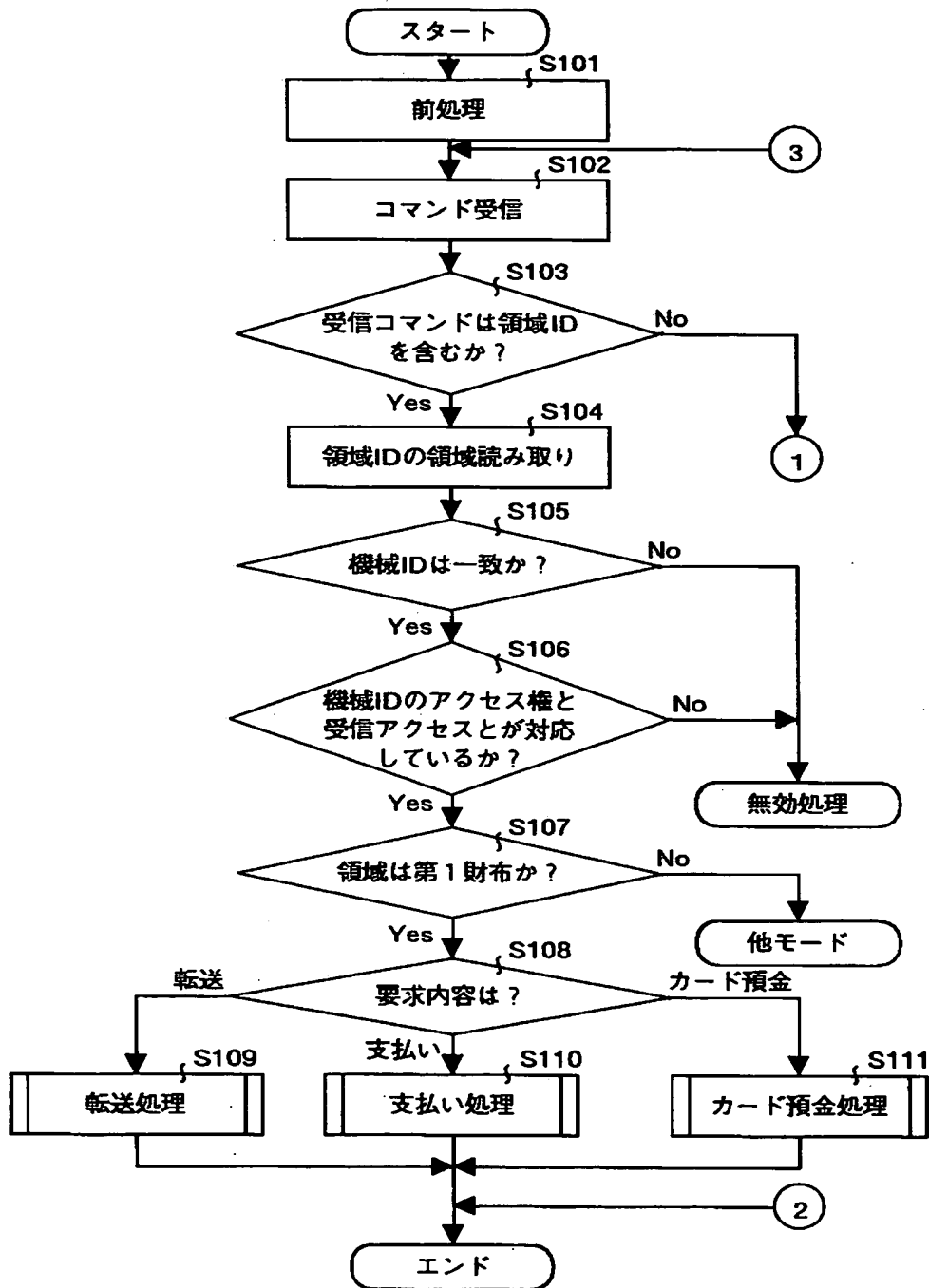




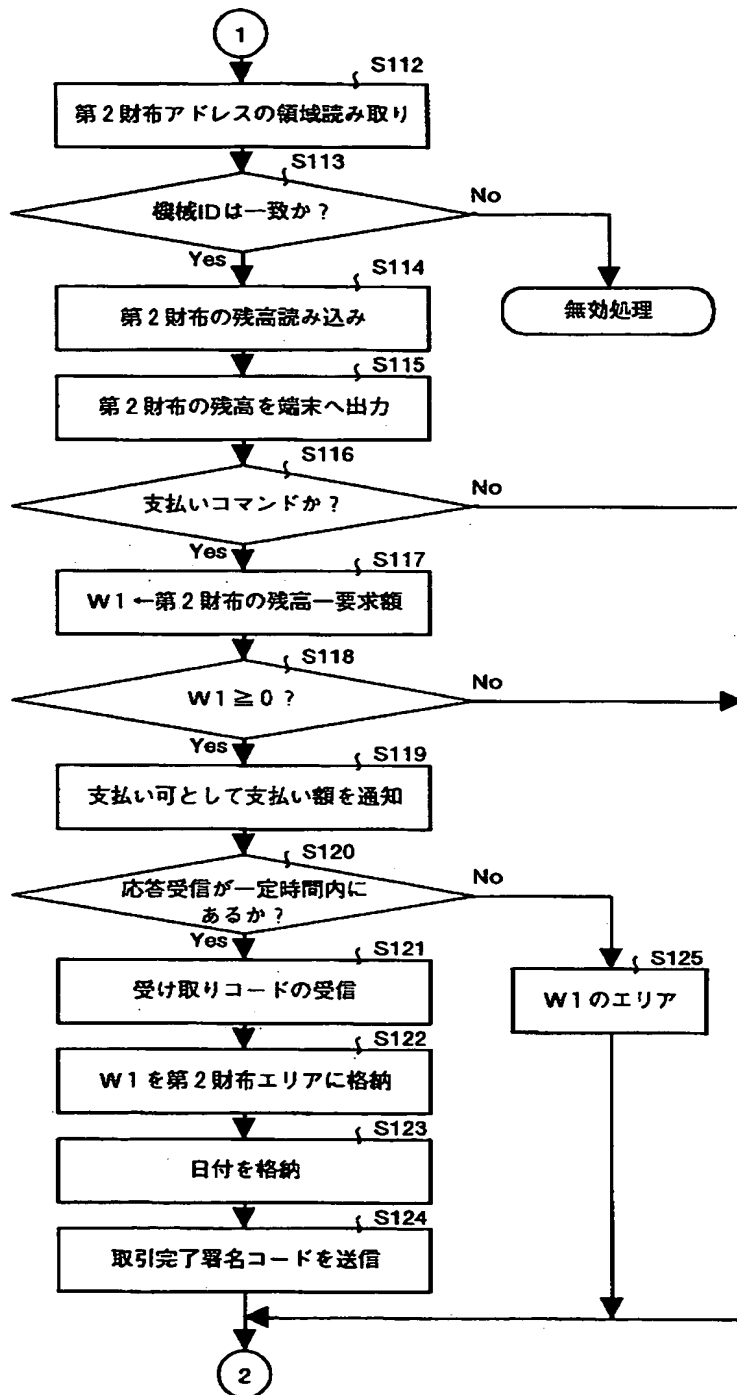
【図7】



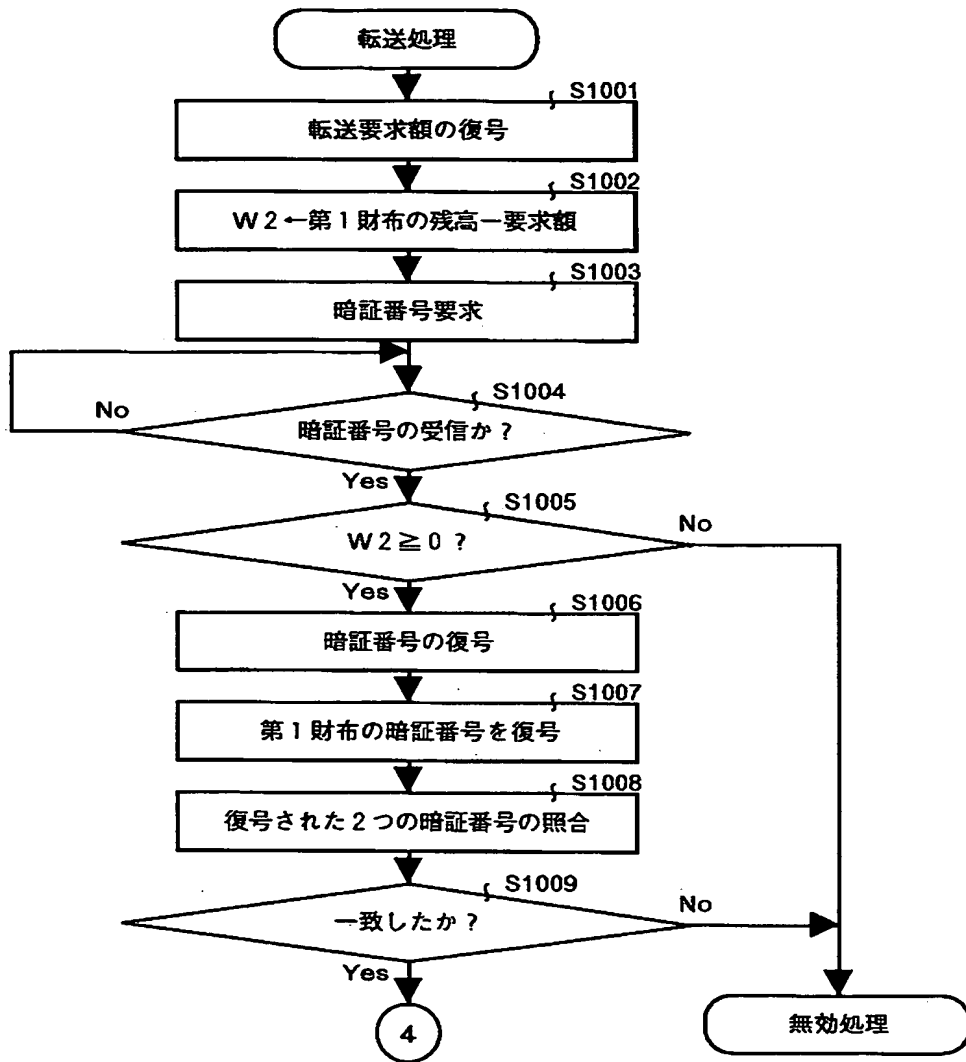
【図 8】



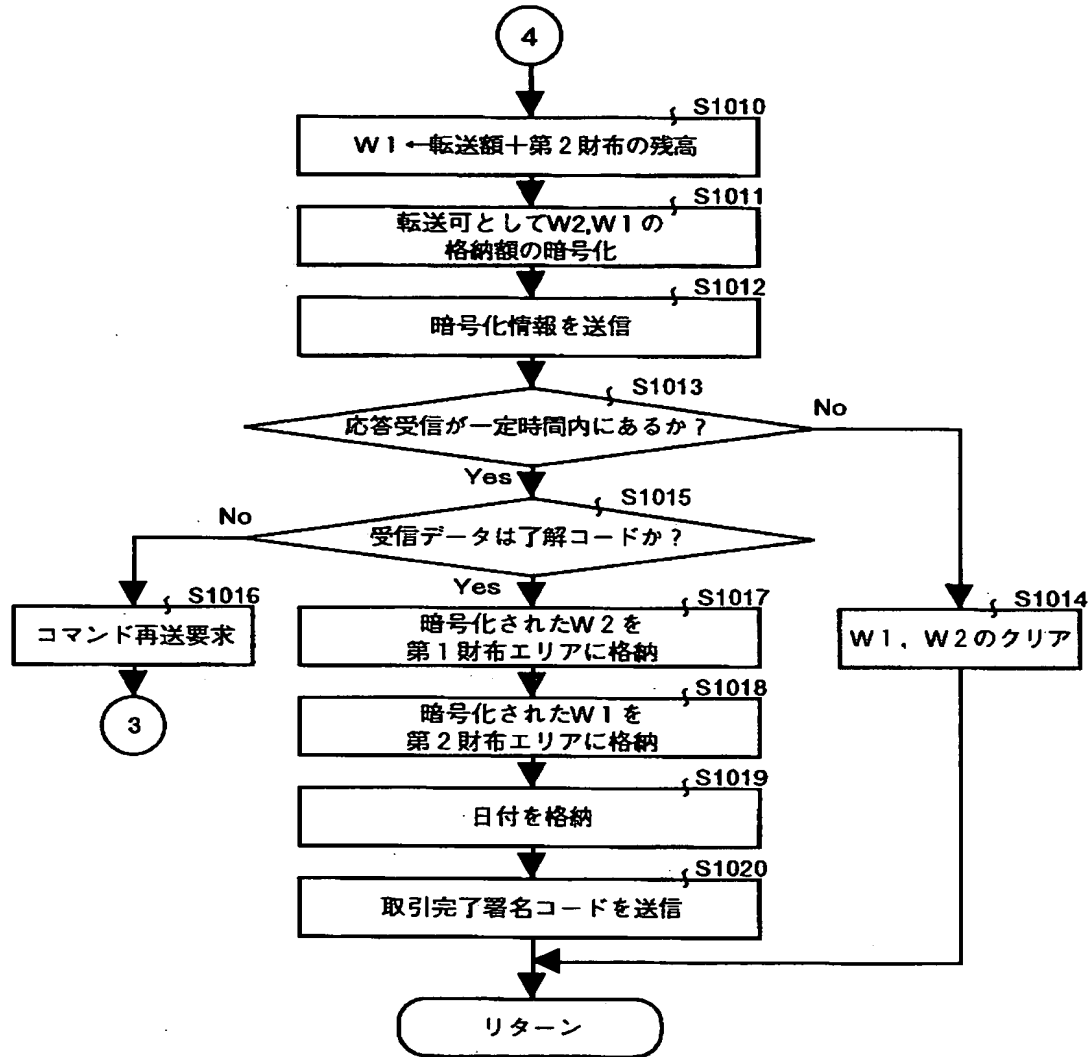
【図9】



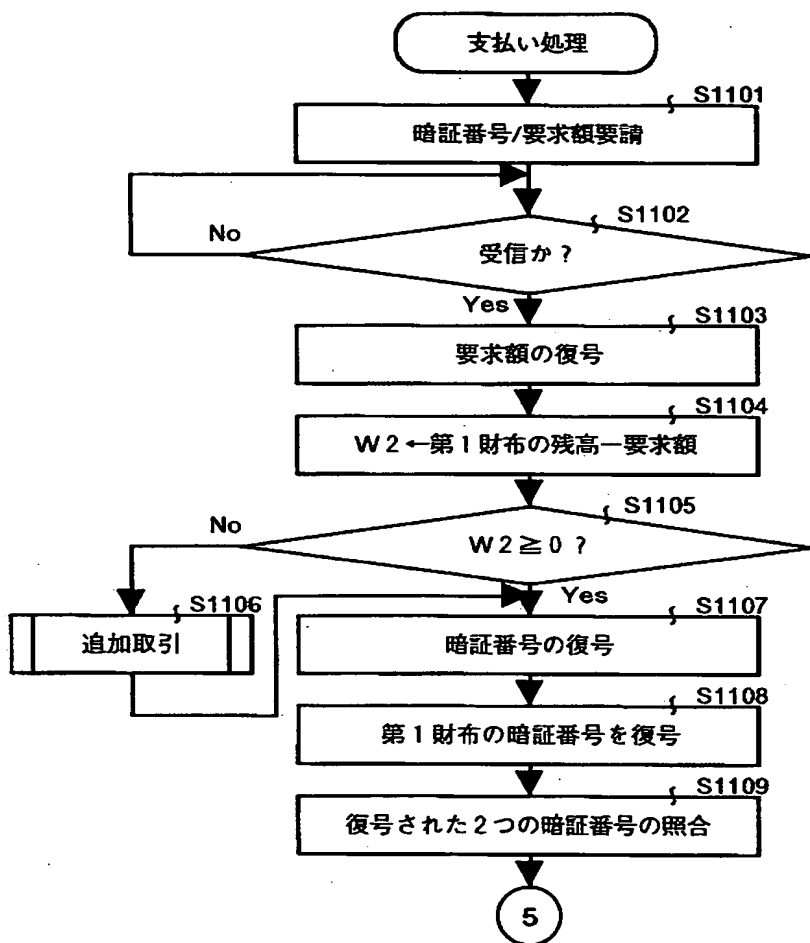
【図10】



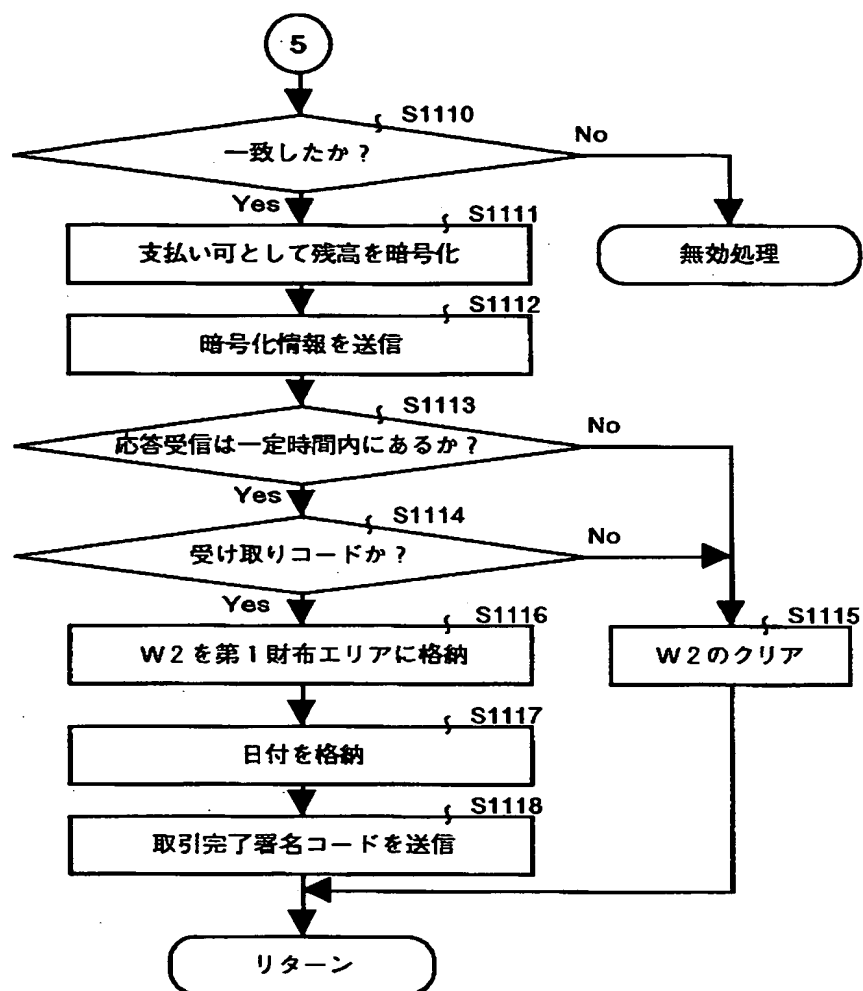
【図 11】



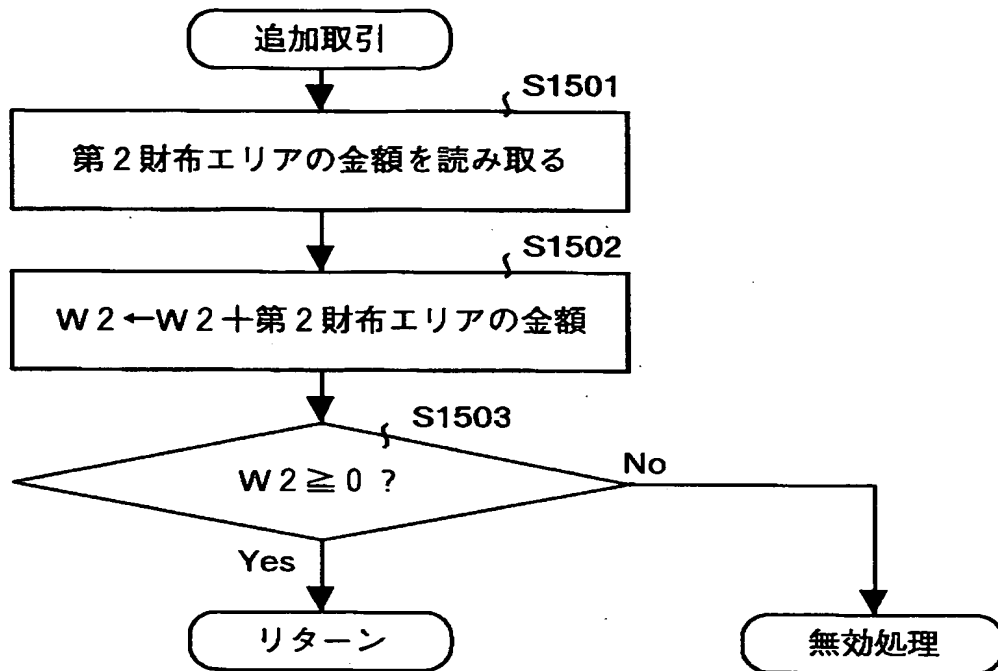
【図12】



【図13】

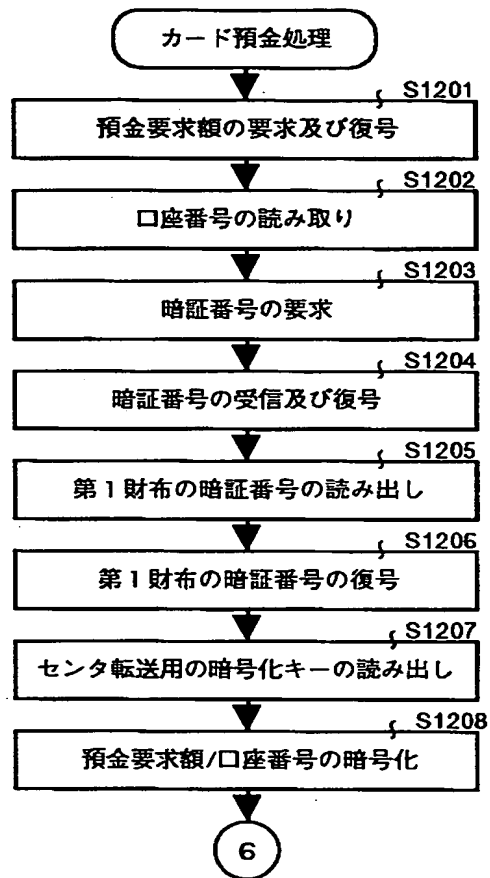


【図14】

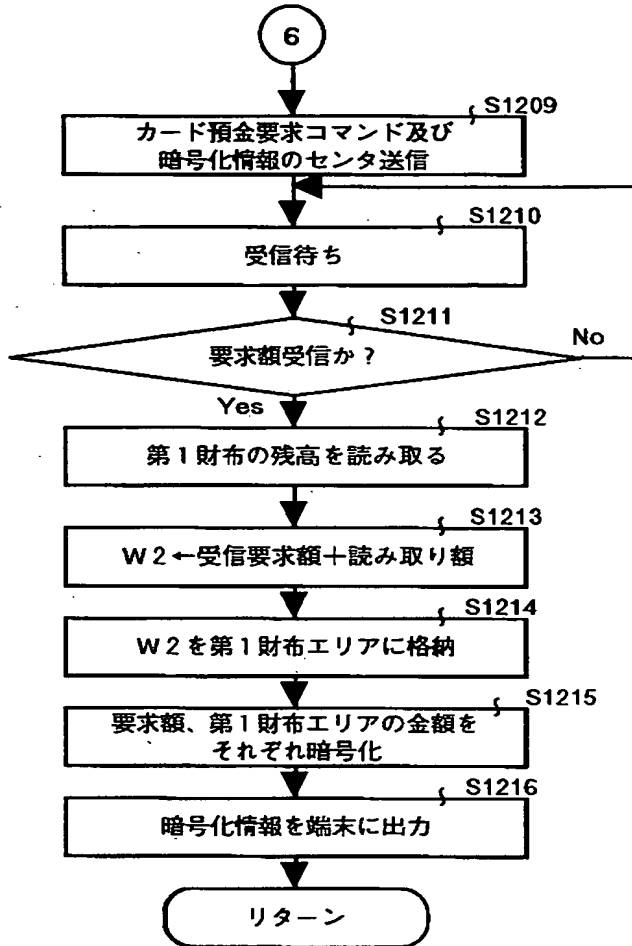




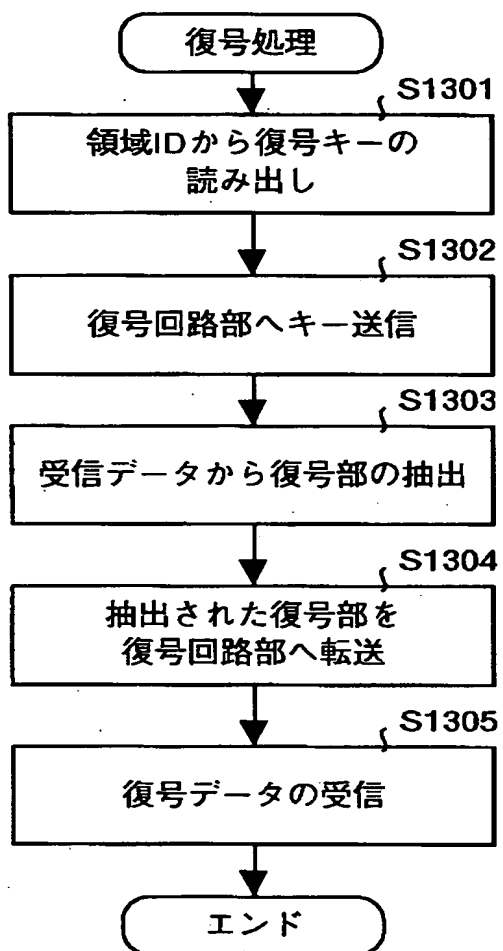
【図15】



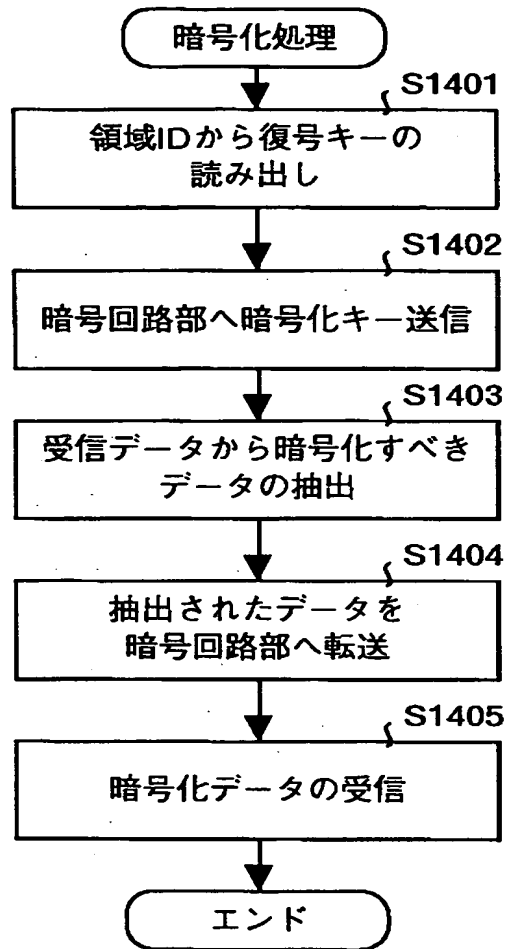
【図16】



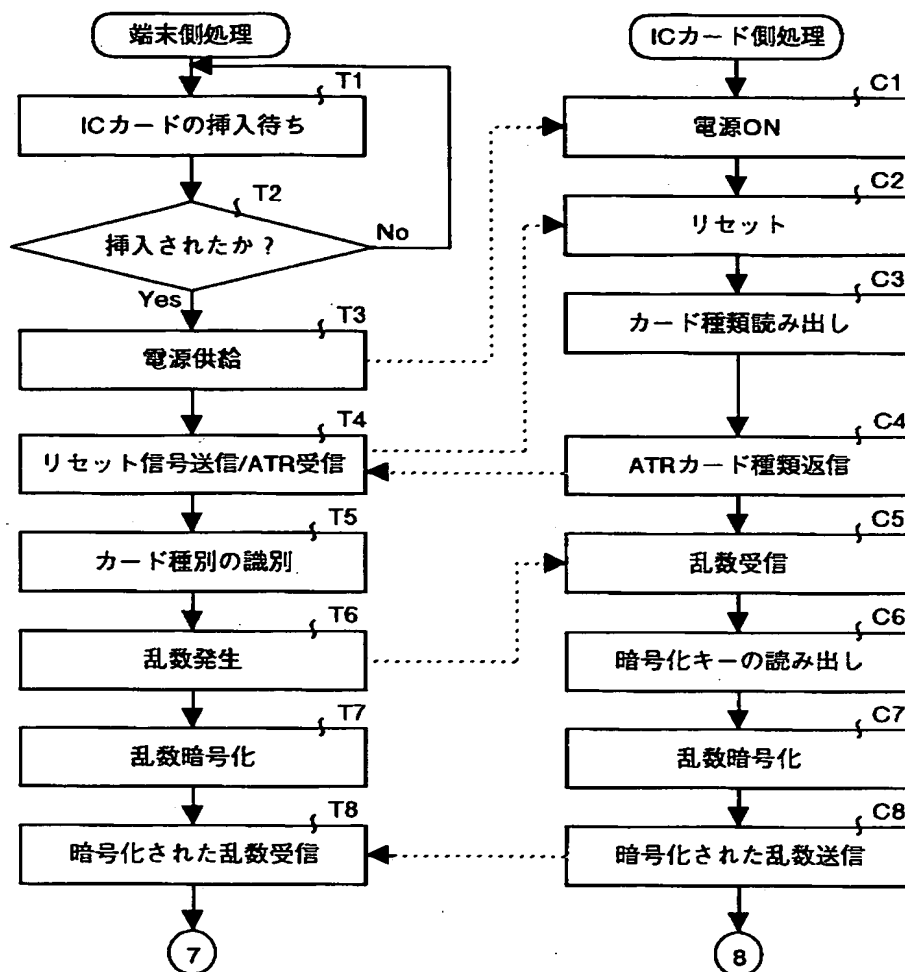
【図17】



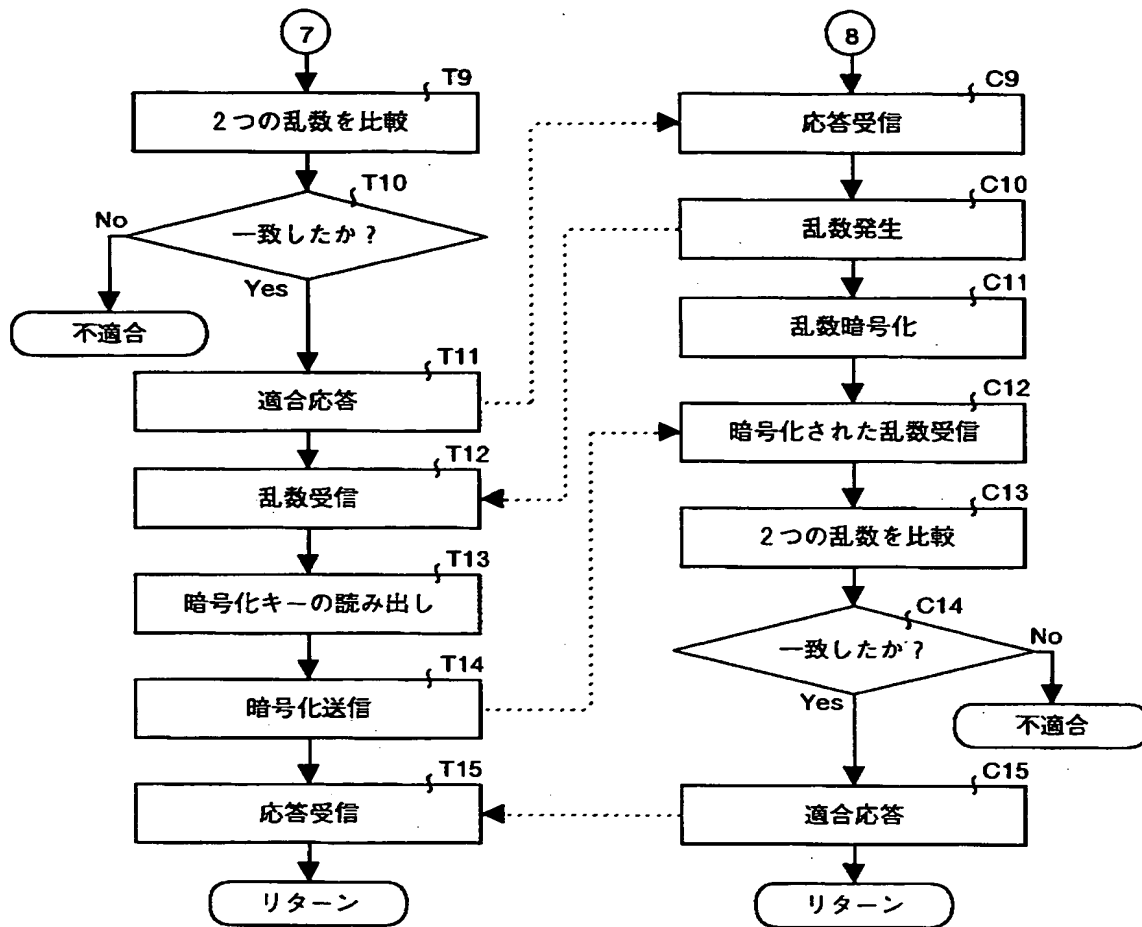
【図18】



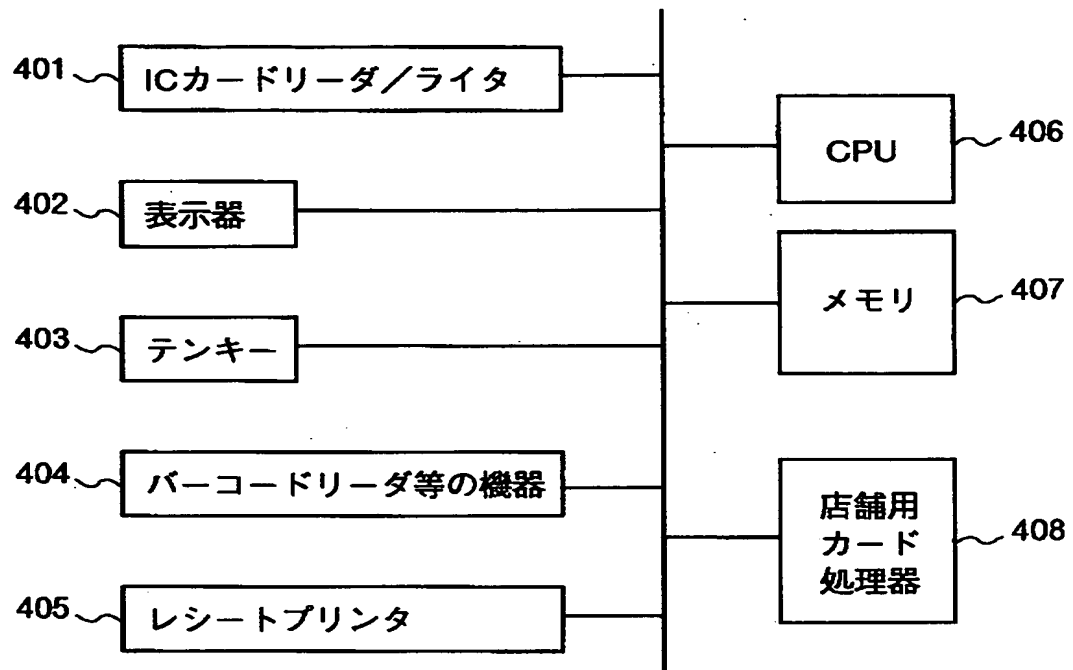
【図19】



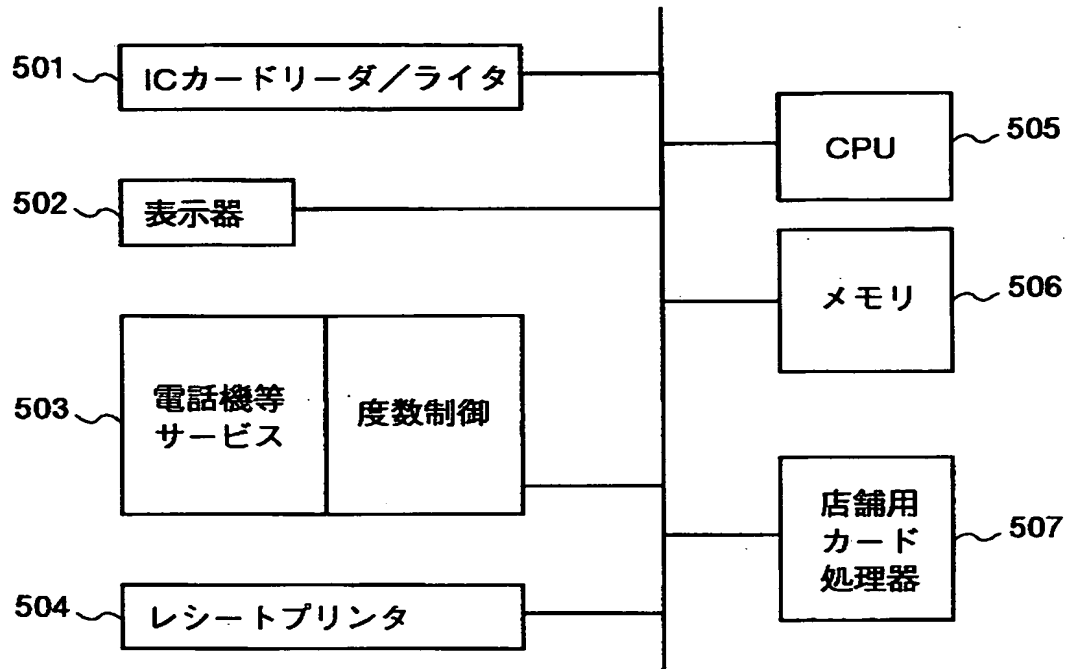
【図20】



【図21】

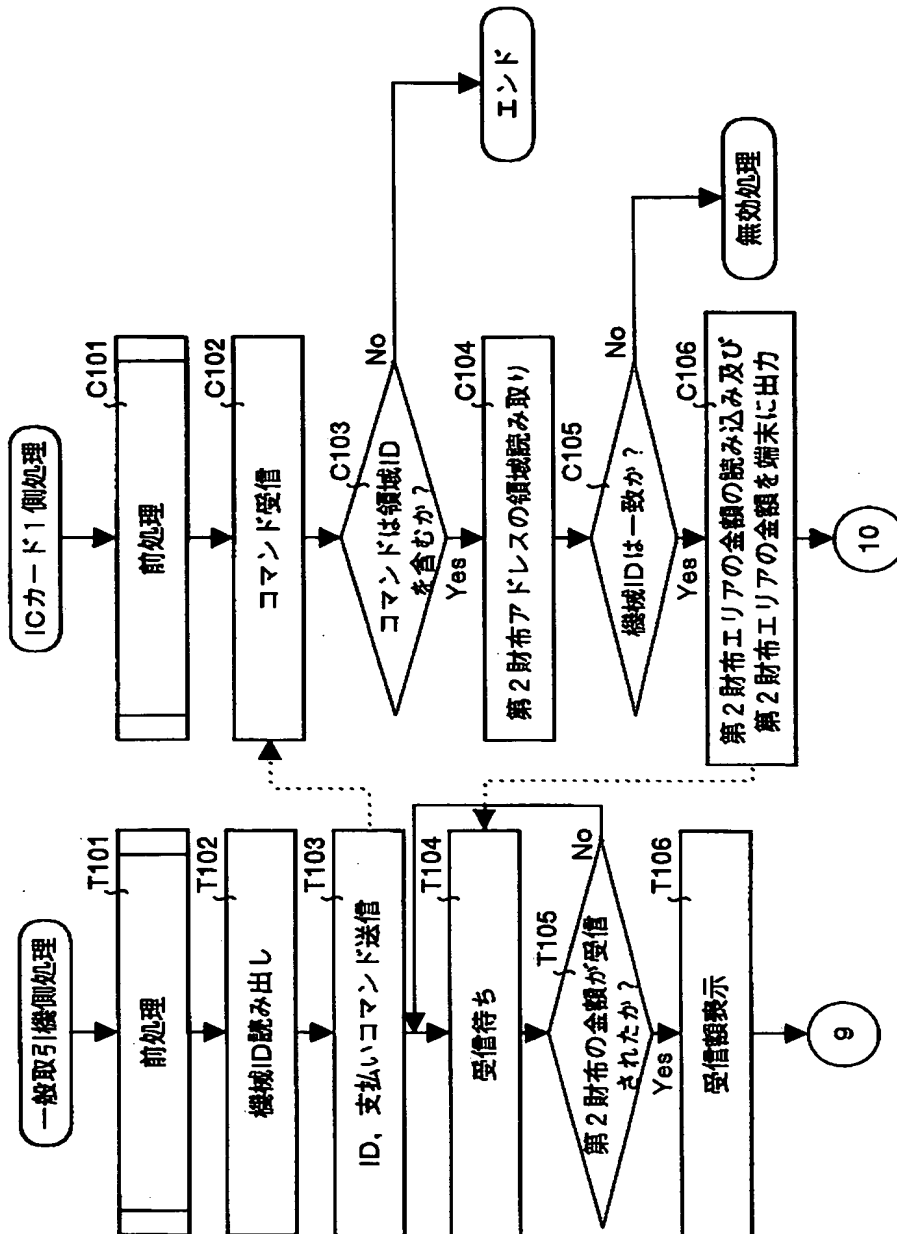


【図 2 2】

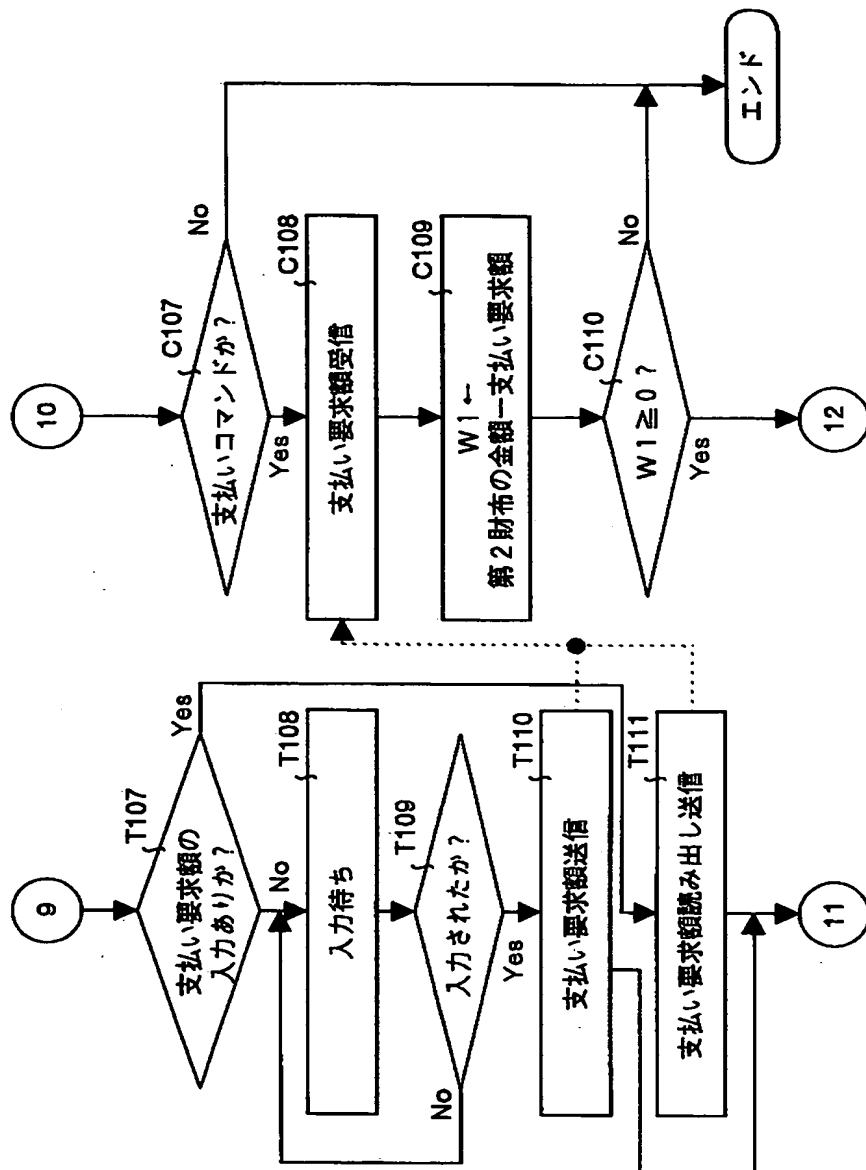




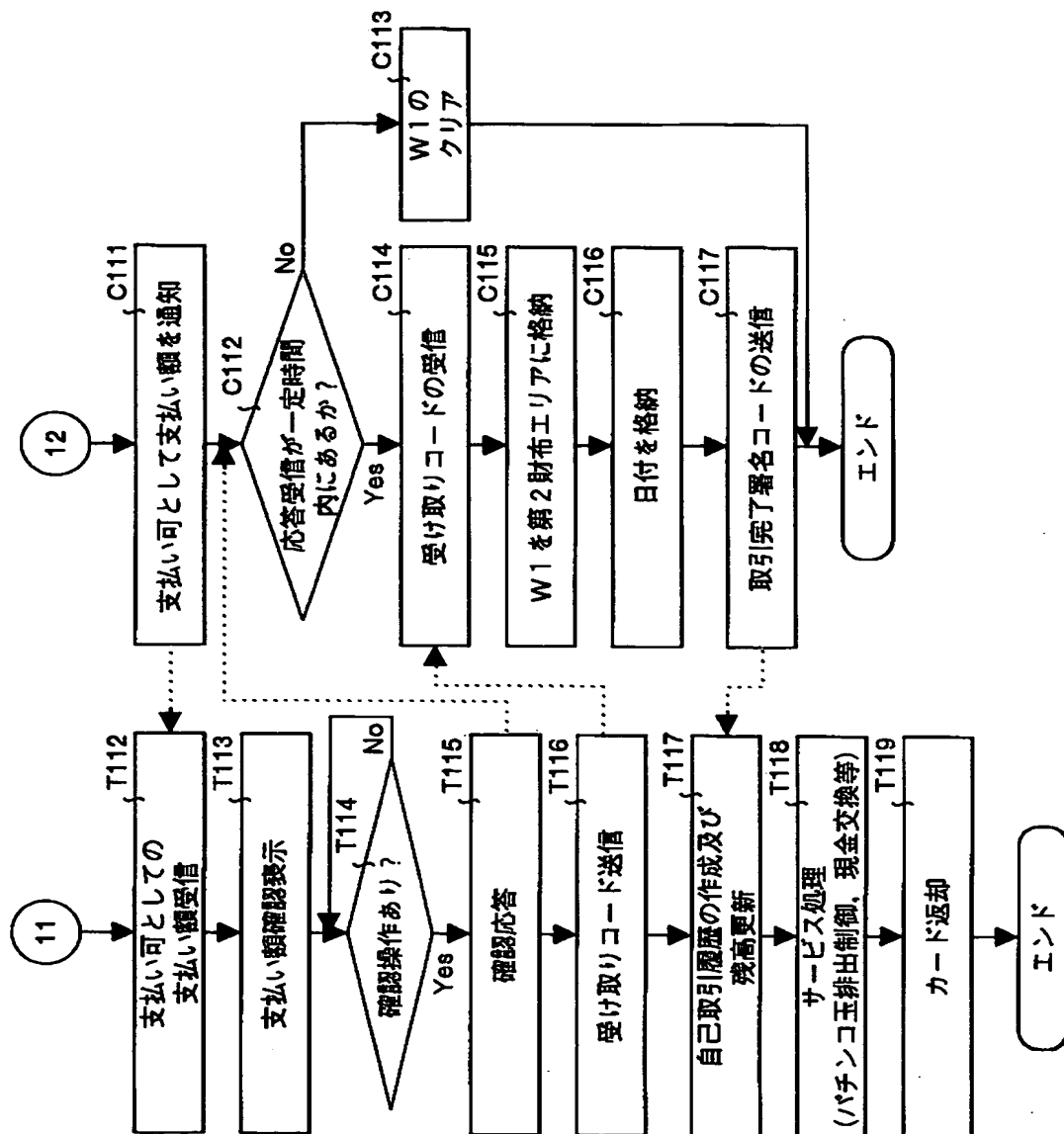
【図23】



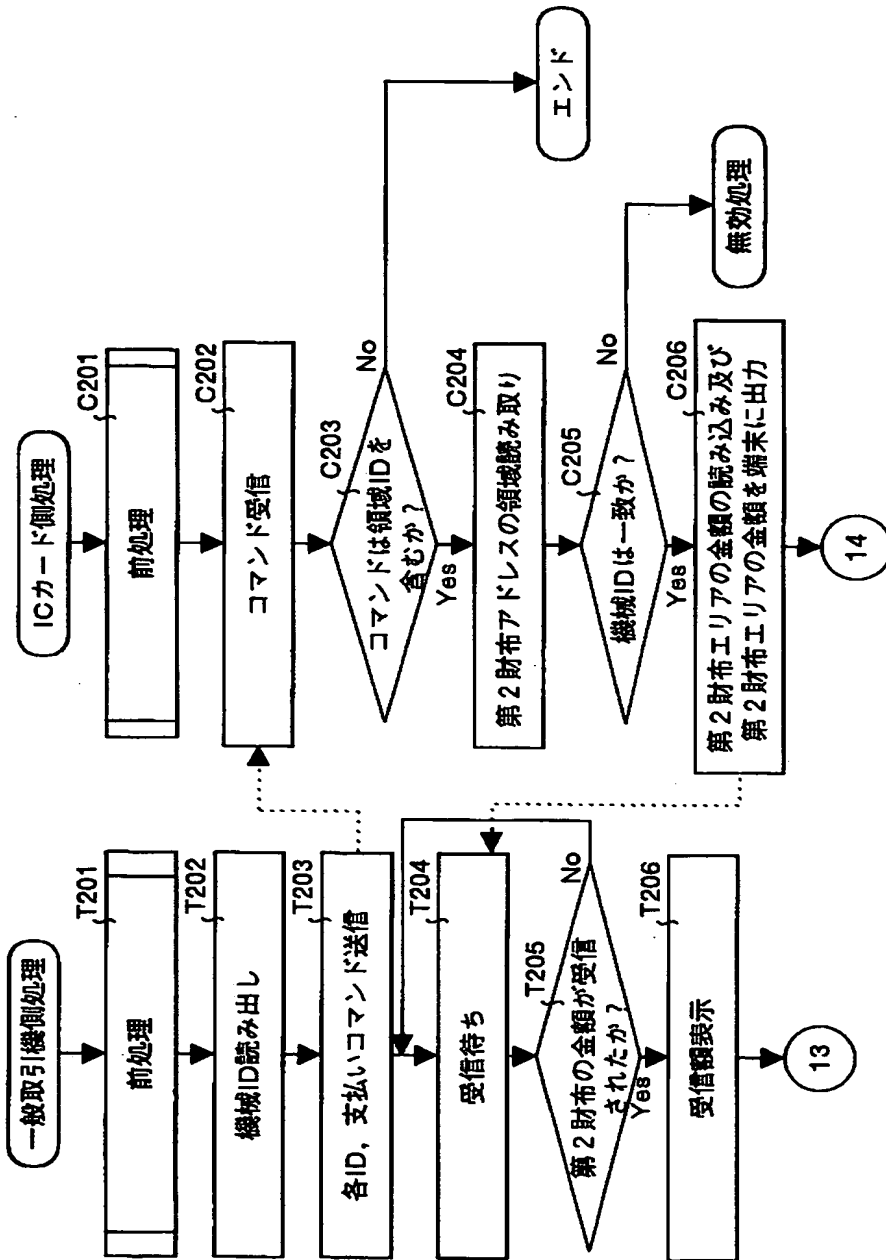
【図24】



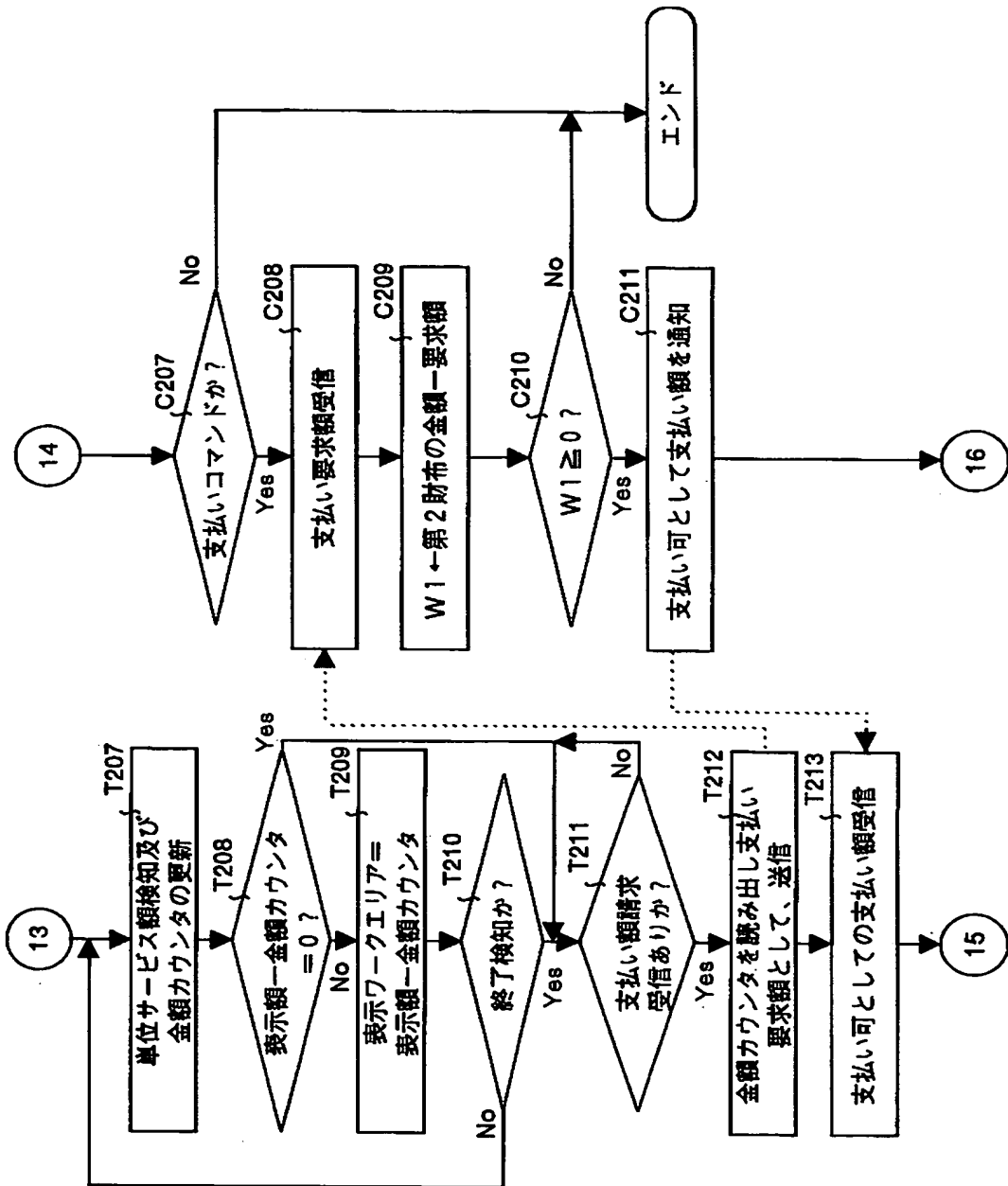
【図25】



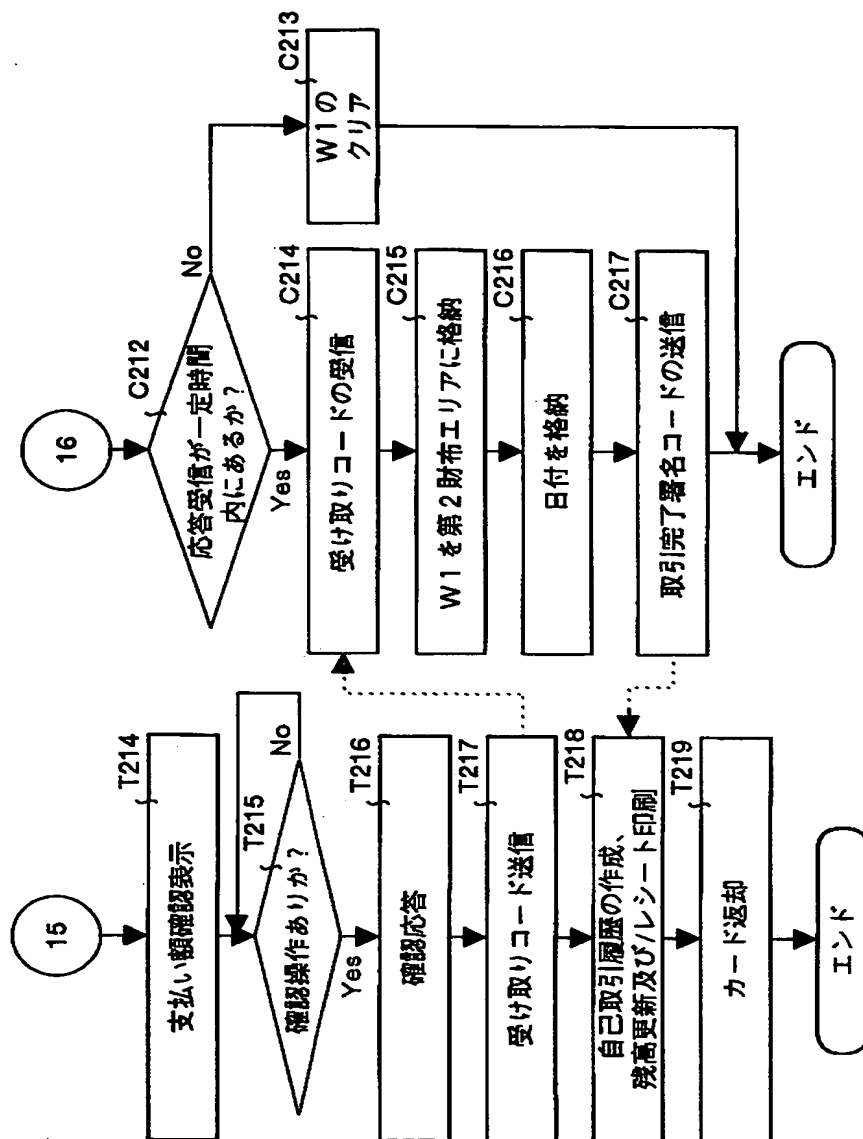
【図26】



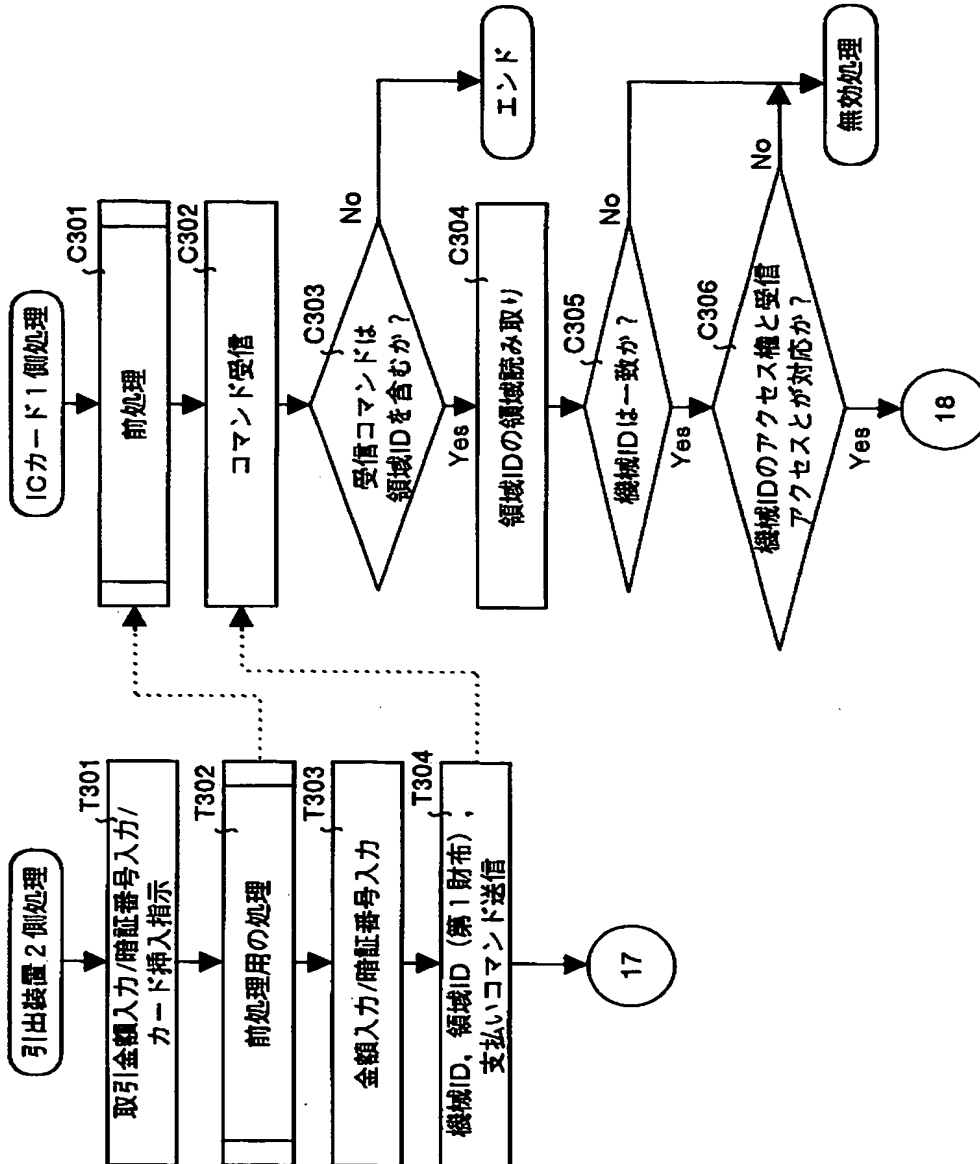
【図 27】



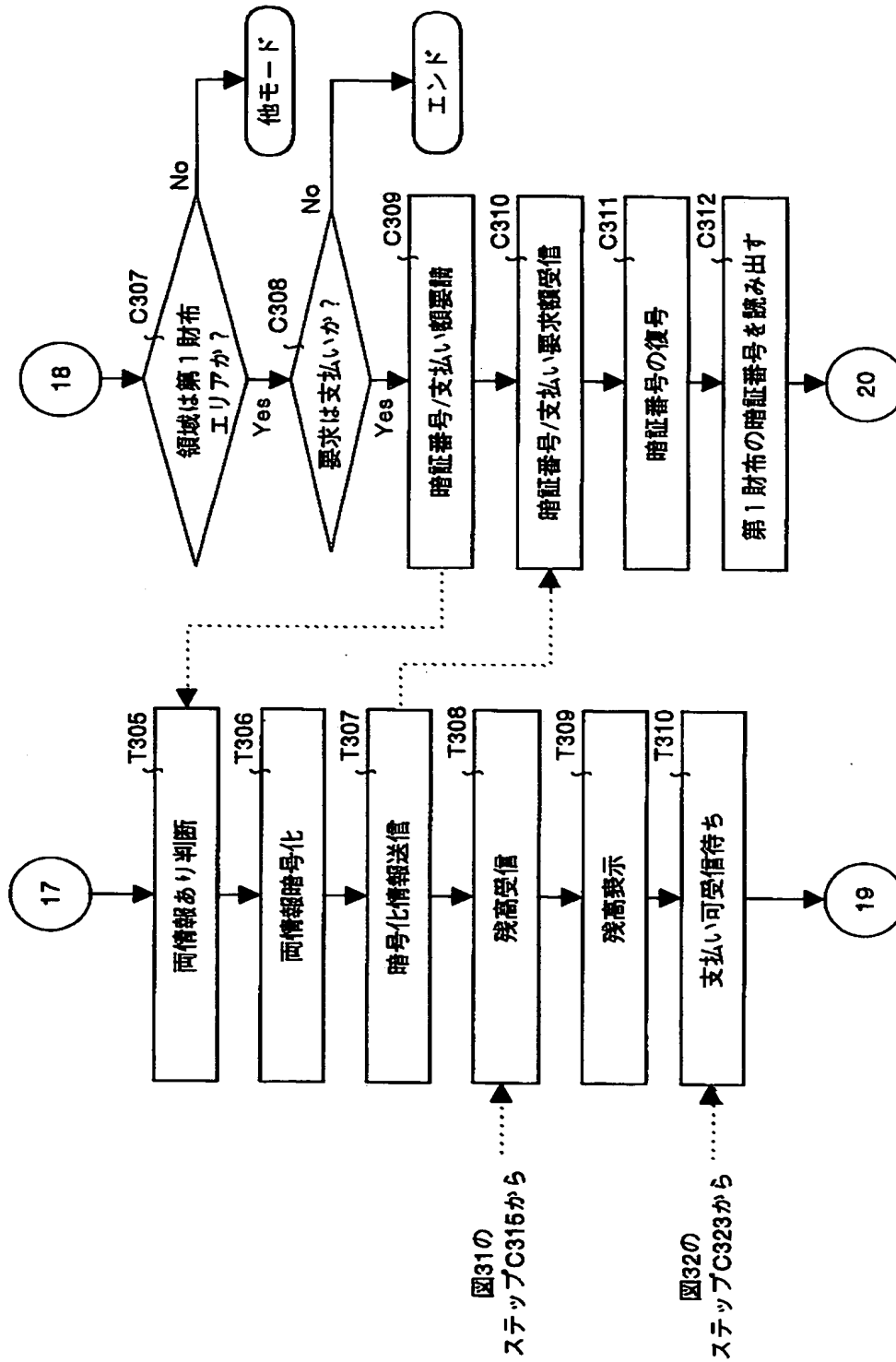
【図 28】



【図29】

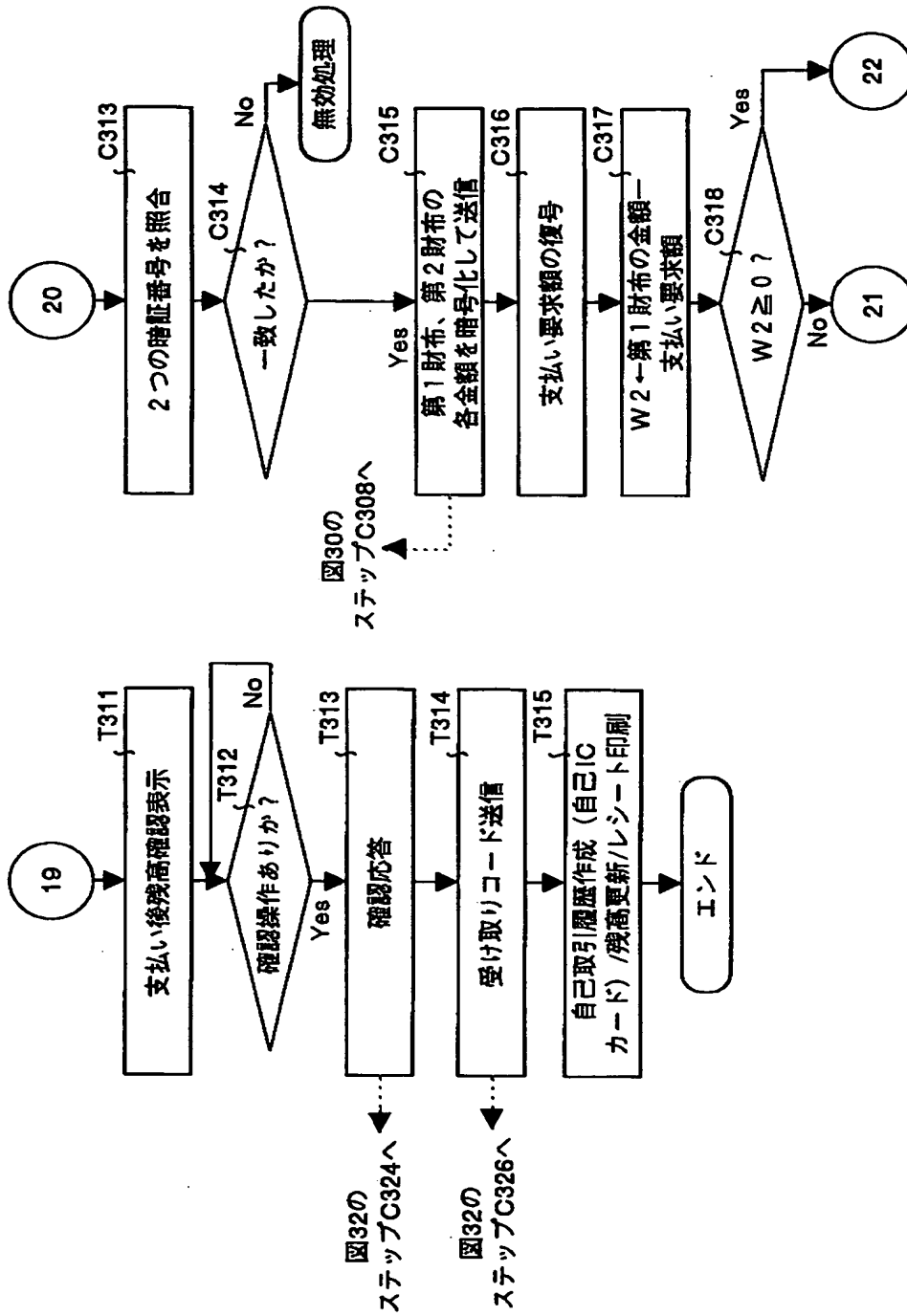


【図30】

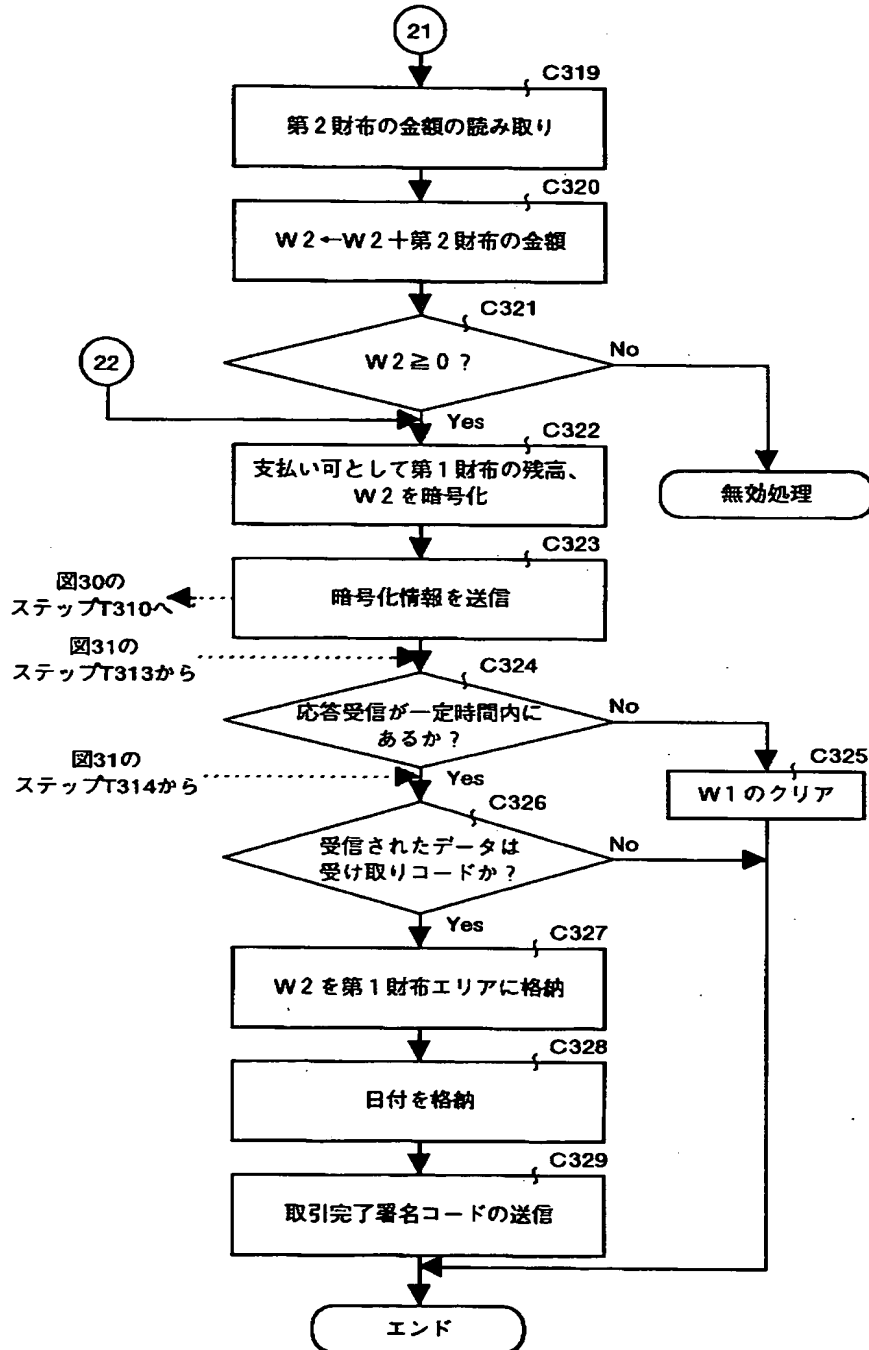




【図 31】



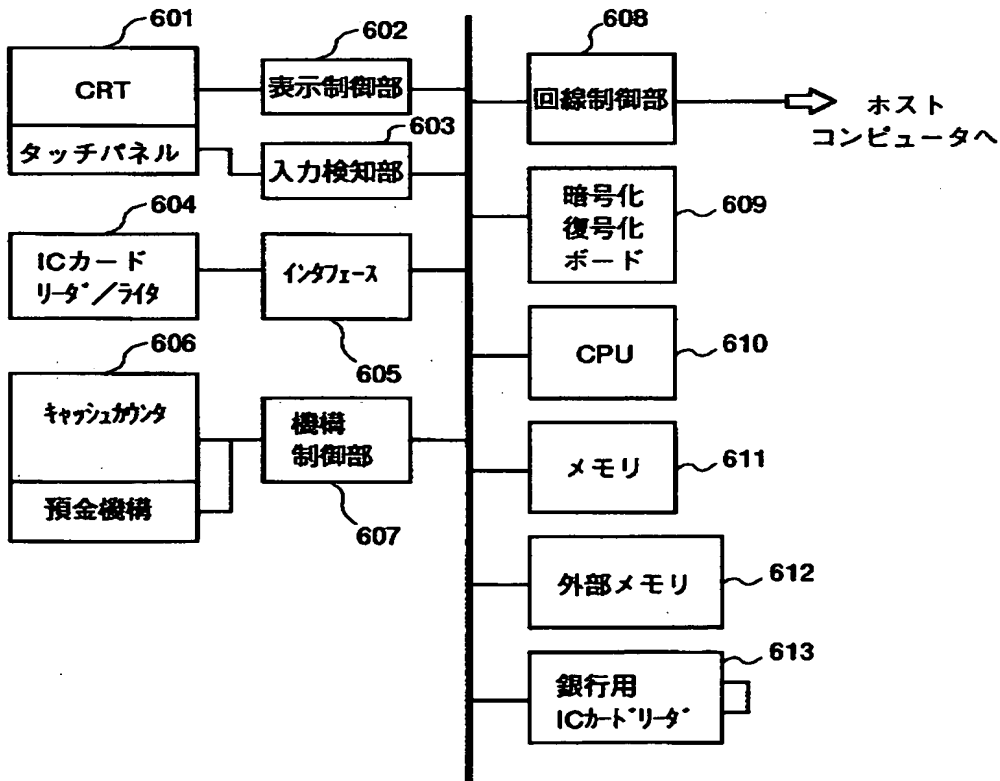
【図32】



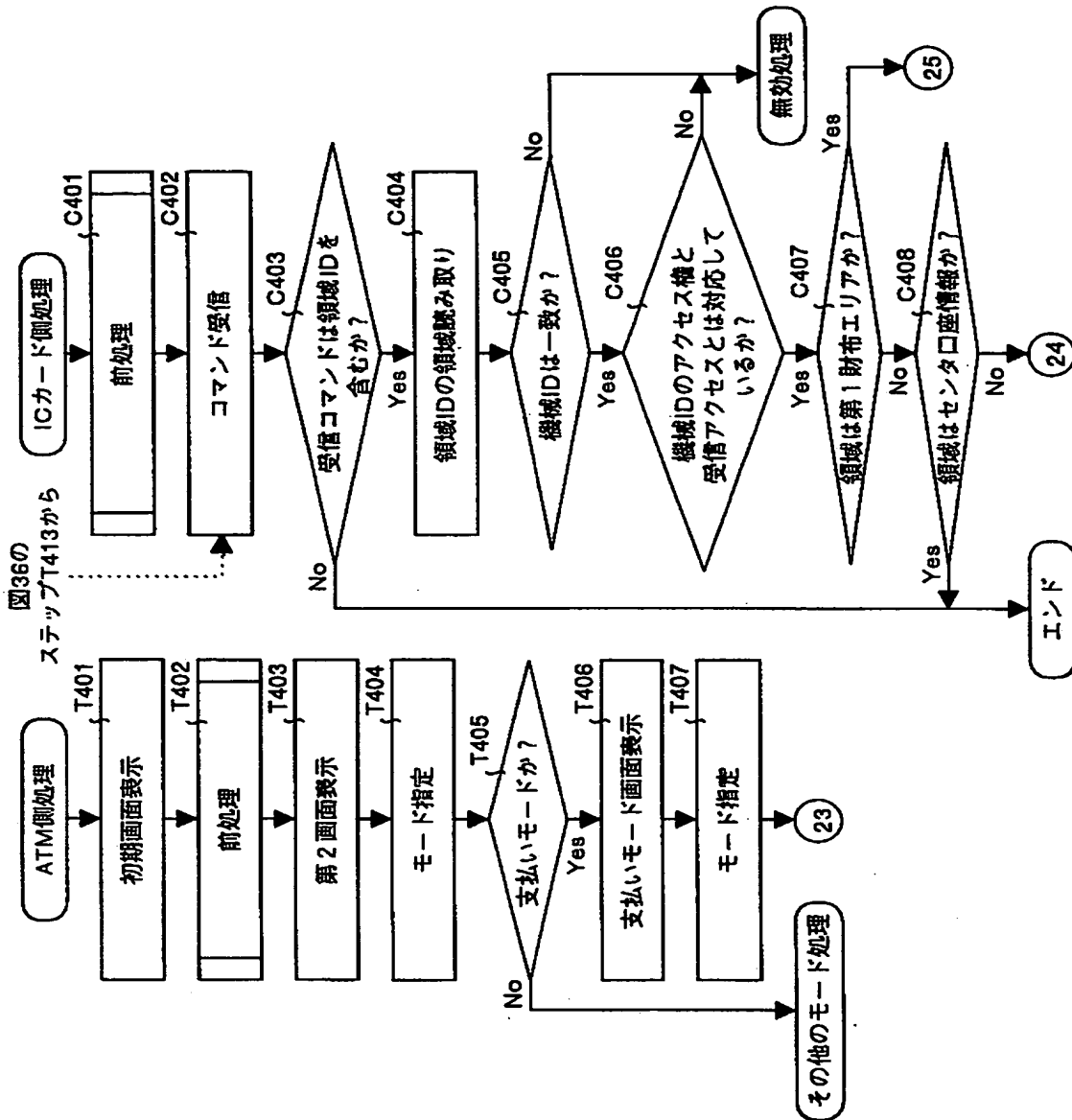
【図33】

	支払い前	支払い後
第1財布	<u>  a  </u> 円	<u>  A  </u> 円
第2財布	<u>  b  </u> 円	<u>  B  </u> 円
支払い額		<u>  C  </u> 円
	<input type="button" value="確認"/> <input type="button" value="取消"/>	

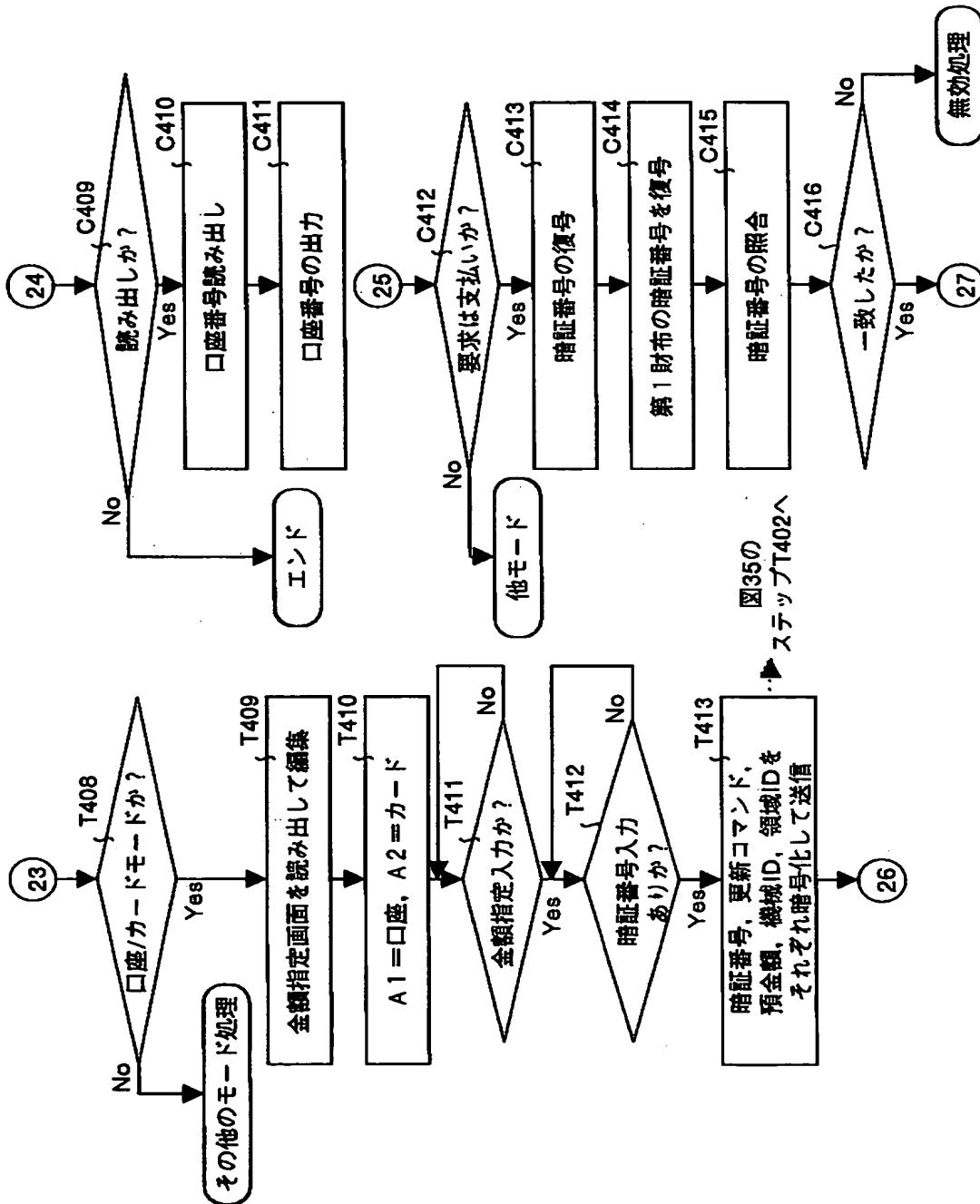
【図34】



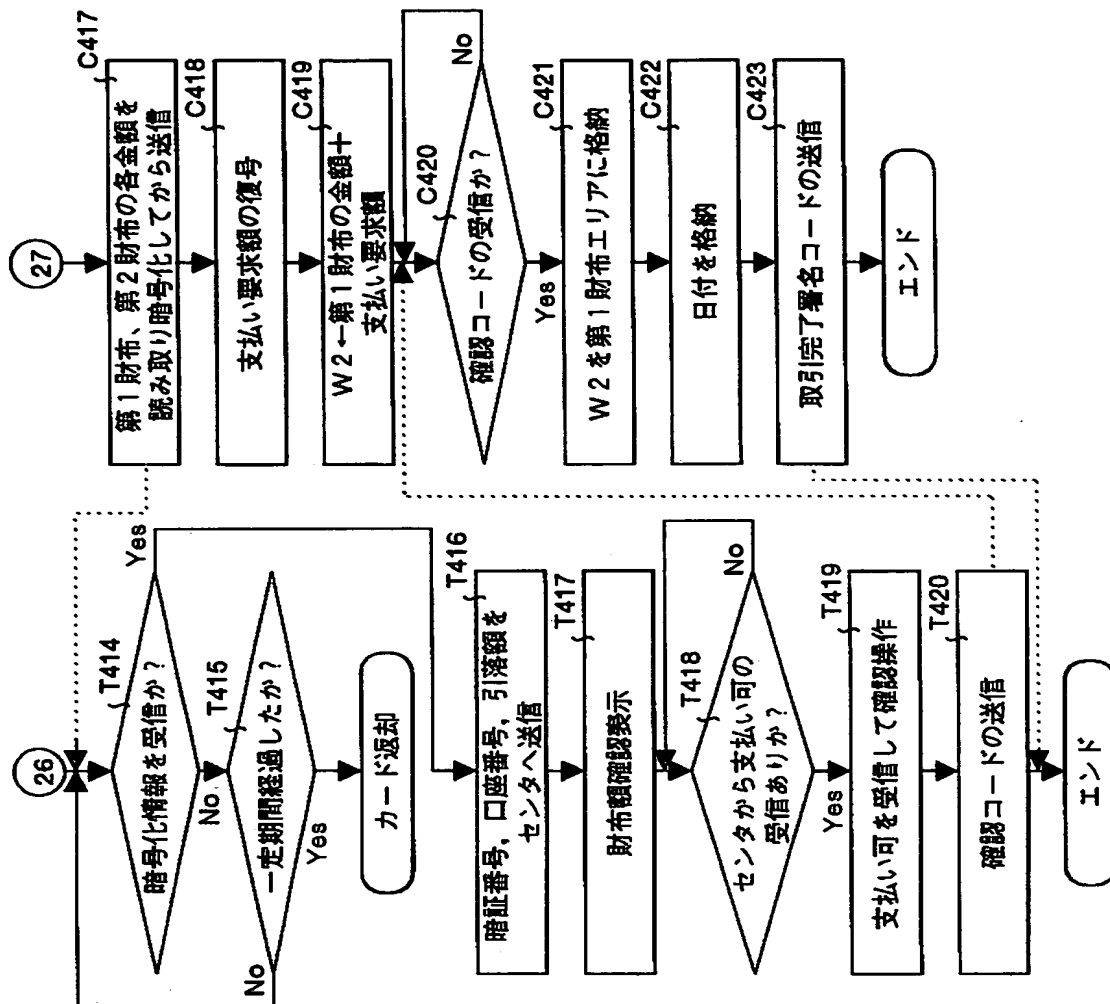
【図35】



【図36】



【図 37】



【図38】

初期画面

(a)

カードを挿入してください。  
暗証番号を入力してください。  
モードを入力してください。

支払	預金	振込	残高照会
----	----	----	------

1	2	3	4	5	6	.....	0
---	---	---	---	---	---	-------	---

支払いモード画面

(b)

モードを選択してください。

口座→カード	口座→現金
カード→カード	カード→現金
口座→カードと現金	
カード→カードと現金	

取消

預金モード画面

(c)

モードを選択してください。

現金をカードへ
現金を口座へ

取消

振込モード画面

(d)

モードを選択してください。

カードから振込先へ
口座から振込先へ

取消

残高照会モード画面

(e)

モードを選択してください。

口座預金残高	両残高
カード残高	

取消

【図39】

(a)

・A1・から・A2・へ引き落とす金額  
を入力してください。

\_\_\_\_\_万\_\_\_\_\_千円

1	2	3	4	5	6	.....	0
---	---	---	---	---	---	-------	---

確認 取消 万円 千円

(b)

	支払い前	支払い後
第1財布	a 円	A 円
第2財布	b 円	B 円
支払い額		C 円

確認 取消

(c)

.....から引き落とす金額を入力して  
ください。

第2財布 ○ \_\_\_\_\_万\_\_\_\_\_千円  
現金 ○ \_\_\_\_\_万\_\_\_\_\_千円

1	2	3	4	5	6	.....	0
---	---	---	---	---	---	-------	---

確認 取消 万円 千円

(d)

	支払い前	支払い後
口座残高		_____円
第1財布	a 円	A 円
第2財布	b 円	B 円
現金支払い額		C 円

確認 取消



【書類名】 要約書

【要約】

【課題】 セキュリティの低い方の財布についてはよりプリペイドカードとしての使い勝手を向上させ、一方、セキュリティの高い方の財布についてはさらにセキュリティを向上させることを課題とする。

【解決手段】 転送装置を用いたセキュリティの高い取引の場合、暗証番号を用いた個人認証を通じてＩＣカードの第１財布（第１財布エリア１０６Ａ）から第２財布（第２財布エリア１０６Ｂ）への預金額の転送を行い、利用装置を用いたセキュリティの低い取引の場合、個人認証を必要とせずに、ＩＣカードの第２財布で利用金額を利用する。

【選択図】 図３

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【代理人】 申請人

【識別番号】 100089118

【住所又は居所】 東京都千代田区霞が関3丁目2番6号 東京倶楽部

ビルディング 酒井国際特許事務所

【氏名又は名称】 酒井 宏明

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社